Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ciencias Matemáticas
Escuela Profesional de Matemática

Sobre la conjetura de Bray-Wilson

TESIS

Para optar el Título Profesional de Licenciado en Matemática

AUTOR

Daniel Alber NINAQUISPE CORALES

ASESOR

Mg. José del Carmen PÉREZ ARTEAGA

Lima, Perú

2020

Referencia bibliográfica

Ninaquispe, D. (2020). *Sobre la conjetura de Bray-Wilson*. Tesis para optar el Título Profesional de Licenciado en Matemática. Escuela Profesional de Matemática, Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

Código ORCID del autor	0000-0001-8790-7489
DNI o pasaporte del autor	44579932
Código ORCID del asesor	0000-0002-7738-5119
DNI o pasaporte del asesor	09489641
Grupo de investigación	Ninguno
Agencia financiadora	Autofinanciado
Ubicación geográfica donde se desarrolló la investigación	Lugar: Sector 2, Grupo 21A, Manzana I, Lote 18. Villa El Salvador. Lima – Perú Coordenadas geográficas: 12°12'27.50" S, 76°57'03.0 O / -12.2076407, -76.9530297
Disciplinas OCDE	1.01.01 -- Matemáticas puras URI: http://purl.org/perepo/ocde/ford#1.01.01

Nota: tomar en cuenta la forma de llenado según las precisiones colocas en la web.
https://sisbib.unmsm.edu.pe/archivos/documentos/recepcion_investigacion/Hoja%20de%20metadatos%20complementarios_30junio.pdf

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE CIENCIAS MATEMATICAS
Ciudad Universitaria – Av. Venezuela S/N cuadra 34
Teléfono: 619-7000, Anexo 1610
Correo Postal: 05-0021, E-mail: eapmat@unmsm.edu.pe
Lima – Perú

Escuela Profesional de Matemática

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN MATEMÁTICA

En la UNMSM - Ciudad Universitaria - Facultad de Ciencias Matemáticas, siendo las 15:00 horas del Viernes 14 de agosto del 2020, se reunieron los docentes designados como Miembros del Jurado Evaluador de Tesis: Dr. Jorge Alberto Coripaco Huarcaya (PRESIDENTE), Mg. Frank Collantes Sánchez (MIEMBRO) Y EL Mg. José del Carmen Pérez Arteaga (MIEMBRO ASESOR), para la sustentación de la tesis titulada: «SOBRE LA CONJETURA DE BRAY-WILSON», presentado por el señor Bachiller Daniel Alber Ninaquispe Corales, para optar el Título Profesional de Licenciado en Matemática.

Luego de la exposición del tesista, el Presidente del Jurado invitó a dar respuestas a las preguntas que le formulen.

Hecha la evaluación correspondiente por los Miembros del Jurado, el tesista mereció la aprobación unánime obteniendo como calificativo promedio la nota de:

Diecisiete (17) (Sobresaliente)

A continuación, el Presidente del Jurado, Dr. Jorge Alberto Coripaco Huarcaya, manifestó que el señor Bachiller DANIEL ALBER NINAQUISPE CORALES, en vista de haber aprobado la sustentación de su tesis, será propuesta para que se le otorgue el Título Profesional de Licenciado en Matemática.

Siendo las 16:10 horas se levantó la sesión firmando para constancia la presente Acta en tres (3) copias originales.

DR. JORGE ALBERTO CORIPACO HUARCAYA
PRESIDENTE

MG. FRANK COLLANTES SÁNCHEZ
MIEMBRO

MG. JOSÉ DEL CARMEN PÉREZ ARTEAGA
MIEMBRO ASESOR

FICHA CATALOGRÁFICA

NINAQUISPE CORALES, DANIEL ALBER

Sobre la conjetura de Bray-Wilson, (Lima) 2020.
VIII, 88 p., 29.7 cm, (UNMSM, Licenciado, Matemática, 2020).
Tesis, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas
1. Matemática. UNSMSM/FdeCM II. Título (Serie).

A mis padres, Teodora y Arcadio, que con tanto esfuerzo y trabajo, me han dado más, de lo que pueda yo retribuirles.

AGRADECIMIENTOS

Agradezco a mi Asesor, el Mg. José Pérez Arteaga, por su apoyo en este trabajo y cuyas conversaciones sobre el pasado, presente y futuro de esta noble ciencia; me han servido siempre de motivación durante todo este proyecto.

RESUMEN

SOBRE LA CONJETURA DE BRAY-WILSON

DANIEL ALBER NINAQUISPE CORALES

AGOSTO - 2020

Asesor: Mg. José del Carmen Pérez Arteaga
Título obtenido: Licenciado en Matemática

El álgebra abstracta ha dado muchísimas contribuciones a la matemática contemporánea, resolviendo en el transcurso de sus 200 años de vida, problemas como: *la imposibilidad de la Quíntica*, *el Teorema de Clasificación de los Grupos Simples* y el tan conocido *Último Teorema de Fermat*. Pero más allá de resolver estas interrogantes, algunas de ellas planteadas hace ya muchos siglos (como fue el caso del Último Teorema de Fermat resuelto por el matermático británido Andrew Wiles), quedan muchas otras aún por resolver; así que el camino de las demostraciones, aunque sea muy estrecho, es realmente un camino muy extenso.

Dentro del álgebra abstracta y más precisamente dentro de la teoría de grupos, un tópico importante es el estudio de los *automorfismos de grupos finitos*. Un problema abierto en teoría de automorfismos de grupos finitos se planteaba de esta manera: "*¿El orden de un grupo finito divide al orden de su grupo de automorfismos?*". González-Sánchez y Jaikin-Zapirain consiguieron dar con la respuesta en 2015, la cual resultó ser negativa. Una consecuencia de su trabajo fue refutar la conjetura dada por Bray y Wilson, la cual planteaba la siguiente afirmación: "*Si G es un grupo no nilpotente supersoluble, entonces* $|\mathrm{Aut}G| > \phi(|G|)$*" (2006:2).*

González-Sánchez y Jaikin-Zapirain al final de su artículo *"Finite p-groups with small automorphism group" (2015)*, ellos mencionan que su trabajo también proporciona un contraejemplo a la conjetura planteada por Bray y Wilson. En esta disertación, siguiendo las indicaciones dadas por ellos, corroboraremos que efectivamente, tal conjetura estaba equivocada.

PALABRAS CLAVE: Grupos supersolubles, Grupos nilpotentes, Función ϕ de Euler, p-Grupos finitos, Automorfismos de p-grupos finitos, Grupo de automorfismos, Grupos pro-p uniformes, Grupos profinitos, Cohomología de grupos profinitos.

Lima
Agosto de 2020

ABSTRACT

ON THE BRAY-WILSON CONJECTURE

DANIEL ALBER NINAQUISPE CORALES

AUGUST - 2020

Advisor: Mg. José del Carmen Pérez Arteaga
Obtained Title: Degree in Mathematics

Abstract algebra has given many contributions to contemporary mathematics, solving in the course of its 200 years of life, problems such as: the impossibility of the Quíntica, the classification of finite simple groups and the well known Fermat's Last Theorem. But beyond solving these questions, some of them raised many centuries ago (as was the case of the Fermat's Last Theorem solved by the british mathematician Andrew Wiles), there are many others still to be resolved; so the road of demonstrations, even if it is very narrow, is really a very long road.

Within abstract algebra and more precisely within group theory, an important topic is the study of automorphisms of finite groups. An open problem in finite group automorphism theory was posed in this way: "Does the order of a finite group divide the order of its automorphism group?". González-Sánchez and Jaikin-Zapirain managed to find the answer in 2015, which turned out to be negative. A consequence of their work was to refute the conjecture given by Bray and Wilson, which posed the following statement: "*If G is a non-nilpotent supersoluble group, then* $|\mathrm{Aut}G| > \phi(|G|)$*" (2006:2).*

González-Sánchez and Jaikin-Zapirain at the end of their article "*Finite p-groups with small automorphism group" (2015)*, they mention that this also provides a counterexample to the conjecture raised by Bray and Wilson. In this dissertation, following the indications given by them, we will confirm that such a conjecture was indeed wrong.

KEY WORDS: Supersoluble groups, Nilpotent groups, Euler's totient function, Finite p-groups, Automorphisms of finite p-groups, Automorphism group, Uniform pro-p groups, Profinite groups, Cohomology of profinite groups.

Lima
August 2020

Índice general

Introducción

En palabras de Birkhoff y McLane: "*Se puede definir el álgebra abstracta como el estudio de las propiedades de los sistemas algebraicos que se conservan en los isomorfismos*". (Birkhoff y McLane, 1960:37). Esta disciplina desde su nacimiento en trabajos de matemáticos como Carl Friedrich Gauss (1777-1855), Augustin Louis Cauchy (1789-1857), Niels Henrik Abel (1802-1829) y Évariste Galois (1811-1832); ha marcado una frontera con el álgebra elemental que se estudia en las distintas escuelas del país o del extrangero (más estudiada en el nivel de secundaria que en primaria). La diferencia aparece cuando pasamos de estudiar las soluciones de una ecuación de segundo grado, a analizar el grupo de automorfismos generado por las raices de un polinomio dado. En la actualidad nos encontramos con problemas que ameritan mucho más que realizar unos simples cálculos, y con soluciones que vienen cargadas de nuevas teorías matemáticas. El algebra abstracta es de uso prioritario en cada disciplina matemática, incluso en física se usa; por ejemplo cuando se estudian las *simetrías* de algún sistema específico. Es así que el álgebra abstracta a pasado a ser una de las ramas más importantes de la matemática contemporánea y de la ciencia en general.

El álgebra abstracta como evolución del álgebra elemental nació para poder dar bellas soluciones a problemas fáciles de plantear pero en escencia unos verdaderos monstruos, por ejemplo, tenemos el caso de la imposibilidad de resolver ecuaciones de grado cinco o más; tal problema fue un verdadero dolor de cabeza para los matemáticos del siglo XVI y XVII, se necesitó de un herramienta nueva que desentrañara todo el misterio debajo de esta interrogante. Evariste Galois un matemático revolucionario de la Francia del siglo XIX nos dejó un legado que es el punto de partida del álgebra abstracta (llamada hasta la primera mitad del siglo XX como *álgebra moderna*); hablamos aquí de la teoría de grupos. Este es entonces uno de los puntos de partida para la matemática contemporánea (junto con las ideas de Riemann y su geometría no euclidiana) y coloca a Evariste Galois en la posteridad, ganándose un lugar muy merecido junto a matemáticos de la talla de Gauss, Cauchy y Abel.

Dentro de la teoría de grupos, y una vez definido lo que es un *grupo* (un conjunto no vacío, en el cual encontramos un elemento inverso para cada elemento en él, y también un elemento neutro), podemos definir lo que es un *homomorfismo* de grupos (una aplicación que respete la estructura de ambos) y desde luego un *automorfismo* (un homomorfismo inyectivo y sobreyectivo de un grupo en sí mismo). Una de las interrogantes más complicadas dentro de la rama de grupos finitos es enunciada así: *¿El orden de un grupo finito divide al orden de su grupo de automorfismos*? Fueron González-Sánchez y Jaikin-Zapirain dos matemáticos españoles que dieron con la respuesta en 2015, en su trabajo " Finite p-groups with small automorphism group"; la cuál fue negativa. Incluso con este resultado lograron

también dar una respuesta negativa a la conjetura planteada por Bray y Wilson, que afirmaba lo siguiente: "*Si G es un grupo no nilpotente supersoluble, entonces $|AutG| > \phi(|G|)$" (2006:2).*

Para abordar la prueba de la existencia de un contraejemplo para tal conjetura, debemos apoyarnos justamente en el trabajo de González-Sánchez y Jaikin-Zapirain. Tal trabajo nos dá las pautas y pasos para mostrar la existencia de tal contraejemplo. Pero antes de ir directamente a la demostración, precisamos de un contenido teórico que abarque desde la topología general hasta la cohomología de grupos profinitos.

En el primer capítulo de este trabajo haremos una revisión de grupos topológicos y límites inversos. En el segundo capítulo introducimos los enteros p-ádicos y el grupo de Prüfer. Enseguida, en el tercer capítulo, haremos una revisión sobre los p-grupos finitos y los automorfismos de grupos finitos. En el capítulo cuatro definiremos lo que es un grupo nilpotente y un grupo supersoluble; ya que la conjetura habla directamente de estos dos tipos de grupos. El quinto capítulo aborda varios tópicos relacionados a los grupos profinitos y pro-p. Grupos profinitos son grupos topológicos compactos y totalmente disconexos, que aparecen naturalmente como grupos de Galois de extensiones de cuerpos. Equivalentemente, un grupo profinito es el límite inverso de un sistema inverso de grupos finitos. Un grupo pro-p es el límite inverso de un sistema inverso de p-grupos finitos. En la primera parte del capítulo cinco presentamos la teoría básica de grupos profinitos y grupos pro-p, incluyendo la conexión de grupos profinitos con grupos de Galois. Enseguida, introducimos los grupos pro-p powerful, grupos pro-p de rango finito y grupos pro-p uniformes. Concluimos el capítulo cinco con una introducción al Álgebras de Lie asociadas a los grupos pro-p uniformes. En el capítulo seis presentamos la conexión entre los grupos p-ádicos analíticos y la Teoría de Lie. En el séptimo capítulo haremos una breve revisión de los conceptos y resultados básicos de la cohomología de grupos profinitos, que vamos a usar en la demostración del teorema principal de este trabajo. En el capítulo 8 introducimos el álgebra de Lie nilpotente de Sato; tal álgebra tiene un papel crucial en la construcción de un grupo pro-p uniforme G tal que $\dim(\mathrm{Aut}(G)) < \dim(G)$. En el capítulo 9, demostraremos el Teorema de González-Sánchez y Jaikin-Zapirain, o mas específicamente, vamos a mostrar que existe un p-grupo finito no-abeliano H tal que $|\mathrm{Aut}(H)| < |H|$. Finalmente en el capítulo 10 mostraremos que la Conjetura de Bray-Wilson no es válida en general, modificando la prueba del Teorema 9.1.4 demostrado en el Capítulo 9.

Además del trabajo de González-Sánchez y Jaikin-Zapirain (2015), el cual ha sido nuestra principal guía para la elaboración de esta disertación, hemos usado otras referencias; las cuales serán indicadas al inicio de cada capítulo.

Capítulo 1

Grupos topológicos y límites inversos

Este primer capítulo analiza las nociones de topología, tales como espacios de Hausdorff, espacios disconexos, grupos topológicos y límites inversos. El desarrollo de este capítulo fue obtenido del libro de Jhon S. Wilson 'Profinite groups' (1997, pp: 1-17).

1.1. Espacios topológicos

Un *espacio topológico* es un conjunto X junto con una familia de subconjuntos llamados conjuntos *abiertos*, con las siguientes propiedades:

(i) El conjunto vacío $\emptyset$ y X son abiertos.

(ii) La intersección de dos conjuntos abiertos es un conjunto abierto.

(iii) La unión de una colección de conjuntos abiertos es un conjunto abierto.

El conjunto formado por esos abiertos es llamado una *topología* en X. Un subconjunto de X es llamado *cerrado* si su complemento es abierto. Si Y es un subconjunto de X la cerradura $\overline{Y}$ de Y es la intersección de todos los conjuntos cerrados conteniendo a Y, en particular $\overline{Y}$ es un conjunto cerrado. Un subconjunto Y de X es llamado *denso* en X si $\overline{Y} = X$. Una *vecindad* abierta de un elemento x de X es un conjunto abierto conteniendo x. Una base para la topología en X es una colección $\{U_\lambda \mid \lambda \in \Lambda\}$ de conjuntos abiertos tal que cada conjunto abierto es una unión de algunos de los conjuntos U_λ (Y una base de vecindades abiertas de x es definida similarmente). Cualquier conjunto X puede ser considerado como un espacio topológico en relación a la topología en la cual cada subconjunto es abierto; esta topología es llamada la *topología discreta* en X, y X es llamado entonces un *espacio discreto.*

Si Y es un subconjunto de un espacio topológico X, entonces la colección de todos los subconjuntos de la forma $Y \cap U$ con U abierto en X es una topología en Y; esta topología es llamada la *topología de subespacio*, y en relación a esta topología Y es llamado un *subespacio de* X.

Un espacio topológico X es llamado *compacto* si, para cada familia $\{U_\alpha \mid \alpha \in A\}$ de subconjuntos abiertos cuya unión es X existe una subfamilia finita $\{U_{\alpha_1}, ..., U_{\alpha_n}\}$ cuya unión es X.

Un espacio topológico X es llamado Hausdorff si dados cualesquier dos elementos x e y en X existen dos vecindades U y V de x e y respectivamente tal que $U \cap V = \emptyset$. Un espacio

X es llamado *conexo* si no puede ser escrito como la unión disjunta de dos subconjuntos abiertos no vacíos. Un espacio topológico X se dice *totalmente disconexo* si cada subespacio conexo tiene como máximo un elemento.

Proposición 1.1.1. *Sea X un espacio compacto Hausdorff.*

(a) *Si C, D son subconjuntos cerrados tal que $C \cap D = \emptyset$, entonces existen subconjuntos abiertos U, V tales que $C \subseteq U$, $D \subseteq V$ y $U \cap V = \emptyset$.*

(b) *Sea $x \in X$ y sea A la intersección de todos los subconjuntos de X conteniendo x, los cuales son al mismo tiempo cerrados y abiertos. Entonces A es conexo.*

(c) *Si X es totalmente disconexo, entonces cada conjunto abierto es la unión de conjuntos los cuales son al mismo tiempo cerrados y abiertos.*

Decimos que una aplicación $f : X \to Y$ entre dos espacios topológicos es *continua* si la imagen inversa de un abierto en Y es un abierto en X. Un *homeomorfismo* es una aplicación biyectiva continua donde la aplicación inversa es continua .

Proposición 1.1.2. *Sean X y Y dos espacios topológicos.*

(a) *Cada subconjunto cerrado de un espacio compacto es compacto.*

(b) *Cada subconjunto compacto de un espacio Hausdorff es cerrado.*

(c) *Si $f : X \to Y$ es continua y X es compacto entonces $f(X)$ es compacto.*

(d) *Si $f : X \to Y$ es continua y biyectiva con X compacto y Y Hausdorff entonces f es un homeomorfismo.*

(e) *Si $f : X \to Y$ y $g : X \to Y$ son continuas e Y es Hausdorff entonces $\{x \in X \mid f(x) = g(x)\}$ es cerrado en X.*

Proposición 1.1.3. *Sea X un espacio totalmente disconexo. Entonces para cada x en X, $\{x\}$ es cerrado en X.*

Sea ρ una relación de equivalencia sobre un espacio topológico X, y escribimos X/ρ para el conjunto cociente y q para la aplicación cociente de X para X/ρ. La *topología cociente* sobre X/ρ es la topología cuyos conjuntos abiertos son los subconjuntos V de X/ρ tales que $q^{-1}(V)$ es abierto en X. Se X/ρ tiene la topología cociente entonces la aplicación cociente q es continua.

El *producto cartesiano* (o simplemente *producto*) de una familia $\{X_\lambda \mid \lambda \in \Lambda\}$ de conjuntos es el conjunto $\prod_{\lambda\in\Lambda} X_\lambda$ cuyos elementos son las aplicaciones x de Λ para $\bigcup_\lambda X_\lambda$ con la propiedad que $x(\lambda) \in X_\lambda$ para cada λ. Podemos considerar los elementos de $\prod_{\lambda\in\Lambda} X_\lambda$ como vectores con entradas o coordenadas indexadas por elementos de Λ. Así un elemento típico será escrito como (x_λ). La aplicación proyección $\pi_\lambda : \prod_{\lambda\in\Lambda} X_\lambda \to X_\lambda$ es la aplicación que lleva un elemento $x \in \prod_{\lambda\in\Lambda} X_\lambda$ para el valor $x(\lambda)$. El producto de una familia finita $X_1, ..., X_n$ de conjuntos es denotada por $X_1 \times ... \times X_n$.

Ahora suponga que cada X_λ es un espacio topológico. La *topología producto* en $\prod_{\lambda\in\Lambda} X_\lambda$ tiene como sus conjuntos abiertos todas las uniones de conjuntos de la forma

$$\pi_{\lambda_1}^{-1}(U_1) \cap ... \cap \pi_{\lambda_n}^{-1}(U_n)$$

con n finito, cada λ_i en Λ y U_i abiertos en X_{λ_i}. Por tanto cada aplicación proyección π_λ es continua, de hecho, la topología producto es la menor topología que hace a las aplicaciones proyección continuas.

Sea Z un espacio topológico y $f : Z \to \prod_{\lambda\in\Lambda} X_\lambda$ una aplicación, afirmamos que f es continua si y solo si cada aplicación $\pi_\lambda f$ es continua.

Teorema 1.1.4. *Sea $\{X_\lambda \mid \lambda \in \Lambda\}$ una familia de espacios topológicos.*

(a) *Si cada X_λ es Hausdorff entonces $\prod_{\lambda\in\Lambda} X_\lambda$ es Hausdorff.*

(b) *Si cada X_λ es totalmente disconexo entonces $\prod_{\lambda\in\Lambda} X_\lambda$ es totalmente disconexo.*

(c) (**Teorema de Tychonoff**)*Si cada X_λ es compacto entonces $\prod_{\lambda\in\Lambda} X_\lambda$ es compacto.*

1.2. Grupos topológicos

Definición 1.2.1. Un *grupo topológico* es un conjunto G que es al mismo tiempo un grupo y un espacio topológico y para el cual la aplicación $(x, y) \to xy^{-1}$ de $G \times G$ (con la topología producto) para G es continua.

Si G es un grupo, $g \in G$ e U, V subconjuntos de G, escribimos $Ug = \{ug \mid u \in G\}$, $gU = \{gu \mid u \in G\}$, $U^{-1} = \{u^{-1} \mid u \in U\}$ y $UV = \{uv \mid u \in U, v \in V\}$. Escribimos 1 para el elemento identidad de un grupo. El siguiente Lema contiene algunos resultados elementales sobre los grupos topológicos.

Proposición 1.2.2. *Sea G un grupo topológico y sean x, y elementos de G. Entonces*

(a) *La aplicación $(x, y) \to xy$ de $G \times G$ para G es continua y la aplicación $x \to x^{-1}$ de G para G es un homeomorfismo. Para cada $g \in G$ las aplicaciones $x \to xg$ y $x \to gx$ de G para G son homeomorfismos.*

(b) *Si H es un subgrupo abierto (resp. cerrado) de G entonces cada clase lateral derecha Hg o izquierda gH de H en G es abierta (resp. cerrada).*

(c) *Cada subgrupo abierto de G es cerrado, y cada subgrupo cerrado de índice finito es abierto. Si G es compacto entonces cada subgrupo abierto de G tiene índice finito.*

(d) *Si H es un subgrupo conteniendo un subconjunto abierto no vacío U de G entonces H es abierto en G.*

(e) *Si H es un subgrupo de G y K es un subgrupo normal de G entonces H es un grupo topológico en relación a la topología inducida y G/K es un grupo topológico en relación a la topología cociente; y la aplicación q de G para G/K lleva conjuntos abiertos para conjuntos abiertos.*

(f) *G es Hausdorff si y solo si $\{1\}$ es un subconjunto cerrado de G; y si K es un subgrupo normal de G entonces G/K es Hausdorff si y solo si K es cerrado en G. Si G es totalmente disconexo entonces G es Hausdorff.*

(g) *Si G es compacto y Hausdorff y si C, D son subconjuntos cerrados entonces el conjunto CD es también cerrado.*

(h) *Supongamos que G es compacto y sea $\{X_\lambda \mid \lambda \in \Lambda\}$ una familia de subconjuntos cerrados con la propiedad que, para todos $\lambda_1, \lambda_2 \in \Lambda$ existe un elemento $\mu \in \Lambda$ para el cual $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$. Si Y es un subconjunto cerrado de G, entonces $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

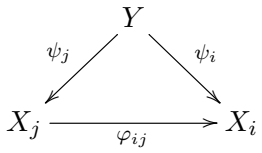
Proposición 1.2.3. *Sea G un grupo topológico compacto. Si C es un subconjunto que es al mismo tiempo cerrado y abierto, y contiene el conjunto $\{1\}$, entonces C contiene un subgrupo abierto normal.*

1.3. Límites inversos

Un conjunto *dirigido* es un conjunto parcialmente ordenado I donde para todos $i, j \in I$ existe un elemento $k \in I$ tal que $i \leq k$ e $j \leq k$.

Definición 1.3.1. Un sistema inverso (X_i, φ_{ij}) de espacios topológicos indexado por un conjunto dirigido I consiste de una familia $\{X_i \mid i \in I\}$ de espacios topológicos y una familia $\{\varphi_{ij} : X_j \to X_i \mid i, j \in I, i \leq j\}$ de aplicaciones continuas tal que φ_{ii} es la aplicación identidad id_{X_i} y $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ donde $i \leq j \leq k$. En la definición no precisamos que los conjuntos X_i sean espacios topológicos. Podemos hacer el cambio por grupos topológicos o anillos, dependiendo de cada caso.

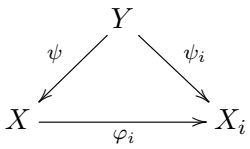
Sea (X_i, φ_{ij}) un sistema inverso de espacios topológicos y sea Y un espacio topológico. Llamaremos a la familia $\{\psi_i : Y \to X_i \mid i \in I\}$ de aplicaciones continuas *compatible* si $\varphi_{ij}\psi_j = \psi_i$ donde $i \leq j$. Esta condición es equivalente a mostrar que el siguiente diagrama



conmuta.

Definición 1.3.2. Un *límite inverso* (X, φ_i) de un sistema inverso (X_i, φ_{ij}) de espacios topológicos (resp. grupos topológicos, anillos) es un espacio (resp. grupos topológicos, anillos) topológico X junto con una familia compatible $(\varphi_i : X \to X_i)$ de aplicaciones continuas (resp. homomorfismos continuos) con la siguiente propriedad universal: siempre que $(\psi_i : Y \to X_i)$ es una familia compatible de aplicaciones continuas del espacio topológico Y (resp. de homomorfismos continuos de un grupo o anillo Y), existe una única aplicación continua (resp. homomorfismo continuo) $\psi : Y \to X$ tal que $\varphi_i\psi = \psi_i$ para cada i.

Por tanto, precisamos que exista un único ψ tal que el siguiente diagrama conmute



La proposición siguiente muestra que el límite inverso existe y es único.

Proposición 1.3.3. *Sea (X_i, φ_{ij}) un sistema inverso de espacios topológicos, indexado por I.*

(a) *Si (Y, φ_i) y (Z, ψ_i) son límites inversos del sistema inverso (X_i, φ_{ij}), entonces existe un isomorfismo $\sigma : Y \to Z$ tal que $\psi_i \sigma = \varphi_i$ para cada i.*

(b) *Denotamos por π_i la aplicación proyección de $\prod_{j\in I} X_j$ para X_i y definimos*

$$X = \{c \in \prod_{j\in I} X_j \mid \varphi_{ij}\pi_j(c) = \pi_i(c), \forall i, j \text{ com } j \geq i\} \tag{1.1}$$

y $\varphi_i = \pi_i|_X$ para cada i. Entonces (X, φ_i) es un límite inverso de (X_i, φ_{ij}).

(c) *Si (X_i, φ_{ij}) es un sistema inverso de grupos topológicos y homomorfismos continuos, entonces X es un grupo topológico y las aplicaciones φ_i son homomorfismos continuos.*

Este resultado muestra que el límite inverso de un sistema inverso (X_i, φ_{ij}) existe y es único bajo isomorfismos. Denotemos este límite inverso por $\varprojlim (X_i, \varphi_{ij})$, o simplemente por $\varprojlim X_i$.

Proposición 1.3.4. Sea (X_i, φ_{ij}) un sistema inverso indexado por I, y escribimos $X = \varprojlim X_i$.

(a) *Si cada X_i es Hausdorff, entonces X es Hausdorff.*

(b) *Si cada X_i es totalmente disconexo, entonces X es totalmente disconexo.*

(c) *Si cada X_i es compacto y Hausdorff, entonces X es compacto y Hausdorff.*

(d) *Si cada X_i es un espacio no vacío compacto Hausdorff, entonces X es no vacío.*

Proposición 1.3.5. *Sea (X, φ_i) un límite inverso de un sistema inverso (X_i, φ_{ij}) de espacios compactos Hausdorff no vacíos indexados por I. Tenemos las siguientes afirmaciones:*

(a) *$\varphi_i(x) = \bigcap_{j\geq i} \varphi_{ij}(x_j)$ para cada $i \in I$ y $x \in X$.*

(b) *Los conjuntos $\varphi_i^{-1}(U)$ con $i \in I$ y U abierto en X_i forman una base para la topología sobre X.*

(c) *Si Y es un subconjunto de X que satisface $\varphi_i(Y) = X_i$ para cada i, entonces Y es denso en X.*

(d) *Si θ es una aplicación del espacio Y para X entonces θ es continua si y solo si cada aplicación $\varphi_i\theta$ es continua.*

(e) *Si $f : X \to A$ es una aplicación continua, siendo A discreto. Entonces para algún i existe una aplicación continua $g : X_i \to A$ satisfaciendo $f = g\varphi_i$.*

Proposición 1.3.6. *Sea X un espacio totalmente disconexo compacto Hausdorff. Entonces X es el límite inverso de sus espacios cocientes discretos.*

Capítulo 2

Los enteros p-ádicos y el grupo de Prüfer

En la segunda sección del capítulo anterior desarrollamos la Teoría de Límites Inversos. Dos ejemplos muy importantes dentro de esta teoría son el anillo de enteros p-ádicos y el grupo de Prüfer. Los enteros p-ádicos serán la base para definir los grupos p-ádicos analíticos en el capítulo 4 y así definir las álgebras de Lie que usaremos en la demostración del teorema principal en el capítulo 7. Para este capítulo fue usado el libro "Field Arithmetic"de Michael D. Fried y Moshe Jarden (2005, pp: 12-15).

2.1. Enteros p-ádicos

Para esta definición de los enteros p-ádicos recurriremos a los límites inversos.

Definición 2.1.1. Sea p un primo. Consideremos los anillos cocientes $\mathbb{Z}/p^i\mathbb{Z}$ y los homomorfismos canónicos $\pi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ definidos por $\pi_{ij}(x+p^j\mathbb{Z}) = x+p^i\mathbb{Z}$ para $j \geq i$. El límite inverso $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$ es el *anillo de enteros p-ádicos*. Este anillo satisface las siguientes propiedades:

(i) Cada $x \in \mathbb{Z}_p$ es una sucesión $(x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ donde $x_i \in \mathbb{Z}$ y $x_j \equiv x_i \mod p^i\mathbb{Z}$, $\forall j \geq i$.

(ii) La aplicación $\rho_i : \mathbb{Z} \to \mathbb{Z}_p$ definida por $\rho_i(a) = (a + p^i\mathbb{Z})_{i\in\mathbb{N}}$ es un homomorfismo inyectivo.

(iii) La sucesión $(x_i)_{i\in\mathbb{N}}$ converge para $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ en la topología p-ádica. Por tanto $\mathbb{Z}$ es denso en $\mathbb{Z}_p$.

(iv) $\mathbb{Z} \neq \mathbb{Z}_p$.

(v) Un elemento $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ de $\mathbb{Z}_p$ es invertible si y solo si $p \nmid x_1$.

(vi) $\mathbb{Z}_p$ es un dominio integral.

Sean $x \in \mathbb{Z}_p$ y los homomorfismos proyección $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, para cada $i \in \mathbb{N}$. En el capítulo de grupos profinitos vamos a ver que un sistema de vecindades para x consiste de

las imágenes inversas $\pi_i^{-1}(x_i + p^i\mathbb{Z})$ para cada $i \in \mathbb{N}$. Así tenemos que

$$\begin{aligned}\pi_i^{-1}(x_i + p^i\mathbb{Z}) &= \{y \in \mathbb{Z}_p \mid \pi_i(y) = x_i + p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i + p^i\mathbb{Z} = x_i + p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i - x_i \in p^i\mathbb{Z}\} \\ &= \{y \in \mathbb{Z}_p \mid y_i \equiv x_i (\mathrm{mod} p^i\mathbb{Z})\}.\end{aligned}$$

Entonces para cada $n \in \mathbb{N}$ tenemos una vecindad básica de x dada por

$$B_n(x) = \{y \in \mathbb{Z}_p \mid y_n \equiv x_n (\mathrm{mod} p^n\mathbb{Z})\}$$

Observación 2.1.2. Los $B_n(x)$ definidos para cada $x \in \mathbb{Z}_p$ definen la *topología p-ádica* para el anillo de enteros p-ádicos.

El homomorfismo $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ es inyectivo. Así podemos ver $\mathbb{Z}$ como un subanillo de $\mathbb{Z}_p$. Si $p \neq 2$, el elemento $(\sum_{i=0}^{n-1} p^i + p^n\mathbb{Z})_{n\in\mathbb{N}}$ está en $\mathbb{Z}_p$ pero no en $\mathbb{Z}$. Se $p = 2$, $(\sum_{i=0}^{n-1} 4^i + p^n\mathbb{Z})_{n\in\mathbb{N}}$ está en $\mathbb{Z}_2$ y no en $\mathbb{Z}$. Así $\mathbb{Z} \subsetneq \mathbb{Z}_p$. Finalmente la sucesión $(x_i)_{i\in\mathbb{N}}$ converge para $(x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ en la topología p-ádica. Entonces $\mathbb{Z}_p = \overline{\mathbb{Z}}$.

Lema 2.1.3. *Sea $\mathbb{Z}_p$ el anillo de enteros p-ádicos.*

(a) *Para cada i, $p^i\mathbb{Z}_p$ es el núcleo de la proyección $\pi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$. Así, $p^i\mathbb{Z}_p$ es un subgrupo abierto de $\mathbb{Z}_p$ de índice p^i.*

(b) *Si H es un subgrupo de $\mathbb{Z}_p$ de índice finito, entonces $H = p^i\mathbb{Z}_p$ para algún $i \in \mathbb{N}$.*

(c) *0 es el único subgrupo cerrado de $\mathbb{Z}_p$ de índice infinito.*

(d) *$p\mathbb{Z}_p$ es el único subgrupo maximal cerrado de $\mathbb{Z}_p$.*

(e) *Todos los subgrupos cerrados no triviales de $\mathbb{Z}_p$ son isomorfos a $\mathbb{Z}_p$.*

Cada elemento $x = (x_i + p^i\mathbb{Z})_{i\in\mathbb{N}}$ de $\mathbb{Z}_p$ tiene una única representación como una serie formal de potencias $\sum_{i=0}^{\infty} a_i p^i$, con $0 \leq a_i < p$ para todo i. Necesariamente, $x_n \equiv \sum_{i=0}^{n-1} a_i p^i$ mód p^n, para cada $n \in \mathbb{N}$.

Lema 2.1.4. *Sea $\alpha : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ un epimorfismo con $n \geq 1$ y H un subgrupo cerrado de $\mathbb{Z}_p$. Supongamos $\alpha(H) = \mathbb{Z}/p^n\mathbb{Z}$. Entonces $H = \mathbb{Z}_p$.*

2.2. El grupo de Prüfer

Definición 2.2.1. Para cada $n \in \mathbb{N}$ consideremos el grupo cociente $\mathbb{Z}/n\mathbb{Z}$ y los homomorfismos canónicos $\sigma_{mn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ definidos por $\sigma_{mn}(x + n\mathbb{Z}) = x + m\mathbb{Z}$, con $m|n$. El límite inverso $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ es el *Grupo de Prüfer*. Este grupo satisface los siguientes items:

(i) La aplicación $\delta_i : \mathbb{Z} \to \hat{\mathbb{Z}}$ definida por $\delta_i(a) = (a + n\mathbb{Z})_{n\in\mathbb{N}}$ es un homomorfismo inyectivo.

(ii) La sucesión $(x_i)_{i\in\mathbb{N}}$ converge para $x = (x_i + n\mathbb{Z})_{n\in\mathbb{N}}$ en la topología p-ádica. Por tanto $\mathbb{Z}$ es denso en $\hat{\mathbb{Z}}$.

(iii) $\hat{\mathbb{Z}}$ es la cerradura del subgrupo generado por 1.

(iv) Vamos a escribir $\hat{\mathbb{Z}} = \langle 1 \rangle$ y decimos que 1 genera $\hat{\mathbb{Z}}$.

(v) Los subgrupos $n\hat{\mathbb{Z}}$ de $\hat{\mathbb{Z}}$ forman una base de vecindades de 0 en la topología inducida.

Lema 2.2.2. *Para cada $n \in \mathbb{N}$, $n\hat{\mathbb{Z}}$ es un subgrupo abierto de $\hat{\mathbb{Z}}$ de índice n y $n\hat{\mathbb{Z}} \equiv \hat{\mathbb{Z}}$. Si H es un subgrupo de $\hat{\mathbb{Z}}$ de índice n, entonces $H = n\hat{\mathbb{Z}}$.*

Lema 2.2.3. *El grupo $\hat{\mathbb{Z}}$ es topológicamente isomorfo al producto cartesiano $\prod \mathbb{Z}_p$ donde p varía en todos los números primos.*

Capítulo 3

p-Grupos finitos

En este capítulo daremos una introducción a los p-grupos finitos, pues ellos desempeñan un papel fundamental en la teoría de grupos finitos y en la teoría de grupos pro-p. Las primeras definiciones son obtenidas del artículo de Gustavo. A. Fernández (2000, pp: 157-165), para desarrollar la parte de automorfismos de grupos finitos usamos el trabajo de David. A. Craven (2008, pp: 14-18) y para los teoremas de Sylow la traducción al español de la publicación de Peter Ludwig Mejdell Sylow (1872). Al final del presente capítulo haremos mención a los artículos que preceden al trabajo de J. González y A. Jaikin (2015) en los cuales se consigue resolver el problema para casos especiales de p-grupos finitos.

3.1. p-Grupos finitos

Definición 3.1.1. Sea p un primo. Un p-grupo finito G es un grupo finito cuyo orden es una potencia de p.

El grupo $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{p-1}\}$ de enteros módulo p con la operación de adición es un grupo cíclico de orden p y por tanto el primer ejemplo de un p-grupo finito. Así tenemos también que para cada $n \in \mathbb{N}$, $\mathbb{Z}/p^n\mathbb{Z}$ es un p-grupo finito.

Sea $\Gamma = \mathrm{GL}_n(\mathbb{Z}_p)$ el grupo de todas las matrices invertibles $n \times n$ sobre $\mathbb{Z}_p$. Definamos

$$\Gamma_i = \{\gamma \in \Gamma \mid \gamma \equiv 1_n (\mathrm{mod} p^i)\},$$

para cada i. Tenemos que $|\Gamma_1 : \Gamma_i| = p^{n^2(i-1)}$. Así los grupos cocientes Γ_1/Γ_i son p-grupos finitos.

Teorema 3.1.2. *Sea G un p-grupo finito y N un subgrupo normal no trivial de G. Entonces $N \cap Z(G) \neq 1$. En particular, el centro de un p-grupo finito no trivial es no trivial.*

Demostración. Observe que G actúa sobre N por conjugación, pues N es normal en G. Tenemos que $|Orb_G(n)| = |G : C_G(n)|$ para cada $n \in \mathbb{N}$ y G es un p-grupo, por tanto la longitud de cada órbita es uma potencia de p. Además, las órbitas de longitud 1 se corresponden a los elementos en N los cuales conmutan con cualquier elemento de G, luego el número de órbitas distintas de longitud 1 es igual a $|N \cap Z(G)|$. Como N es la unión

disjunta de sus orbitas, sigue que

$$|N| = |N \cap Z(G)| + \sum_{i=1}^{r} |Orb_G(n_i)|$$

donde $n_1, ..., n_r$ son los representantes de las órbitas de longitud mayor que 1. Haciendo en la última desigualdad módulo p y considerando que $|N| > 1$, tenemos que

$$|N \cap Z(G)| \equiv 0 \pmod{p}$$

y así sigue que $N \cap Z(G) \neq 1$. □

Corolario 3.1.3. *Sea G un p-grupo finito. Si H es un subgrupo normal de G de orden p entonces H es central en G (i.e. $H \leq Z(G)$) .*

Las siguientes consecuencias del Teorema 3.1.2 son muy importantes en la teoría de p-grupos finitos.

Teorema 3.1.4. *Sea G un p-grupo finito.*

(i) *Si $H \lneq G$ entonces $H \lneq N_G(H)$.* **(la condición del normalizador)**

(ii) *Si M es un subgrupo maximal de G entonces M es normal en G y $|G : M| = p$.*

Demostración. (i) Probaremos esto por inducción sobre $|G|$. El resultado es obvio si $|G| = p$, por eso vamos a suponer que $|G| > p$. Si $Z(G)$ no está contenido en H entonces $H \lneq HZ(G) \leq N_G(H)$ y acabamos. Así podemos suponer que $Z(G) \leq H$. Como $Z(G) \neq 1$, de la hipótesis inductiva obtenemos que $H/Z(G) \lneq N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G)$ y consecuentemente $H \lneq N_G(H)$.

(ii) Si M es maximal en G, obtenemos de (i) que $N_G(M) = G$, esto es, $M \lhd G$. Entonces el grupo cociente G/M es un p-grupo que no posee subgrupos no triviales. Por tanto G/M tiene orden p y $|G : M| = p$. □

El siguiente resultado muestra que los subgrupos de un p-grupo están bastante bien situados.

Teorema 3.1.5. *Sea G un p-grupo finito de orden p^m.*

(i) *Si N es un subgrupo normal de G de orden p^k, entonces existe una serie*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = N \leq ... \leq G_m = G \tag{3.1}$$

tal que $G_i \lhd G$ y $|G_{i+1} : G_i| = p$ para todo i. En particular, un p-grupo tiene subgrupos normales de cada orden posible.

(ii) *Si H es un subgrupo de G de orden p^k, entonces existe una serie*

$$1 = G_0 \leq G_1 \leq ... \leq G_k = H \leq ... \leq G_m = G \tag{3.2}$$

tal que $G_i \lhd G_{i+1}$ e $|G_{i+1} : G_i| = p$ para todo i. Entonces cada subgrupo de un p-grupo es subnormal.

Demostración. (i) Probaremos esto por inducción sobre $|G|$. Supongamos primero que $N \neq 1$. Entonces del Teorema 3.1.2 obtenemos $Z = N \cap Z(G) \neq 1$. Escogiendo cualquier G_1 en Z de orden p. Entonces G_1 es normal en G y el resultado sigue por aplicación de la hipótesis inductiva para G/G_1 y para el subgrupo normal N/G_1. Finalmente, si $N = 1$ entonces podemos tomar cualquiera de las series obtenidas del argumento anterior.

(ii) Primero, recordemos que un subgrupo H de G es subnormal si existe una cadena finita de subgrupos del grupo G donde cada subgrupo de la cadena es normal en el siguiente subgrupo comenzando en H y terminando en G, i.e. si existen $H_0, H_1, ..., H_k \leq G$ tal que

$$H = H_0 \leq H_1 \leq ... \leq H_k \leq G$$

y $H_i \lhd H_{i+1}$, para cada $i = 0, .., k-1$.
Para la prueba usaremos inducción sobre $|G|$. Si $H = G$ entonces podemos usar la parte (i) para obtener la serie buscada. De otra forma H está contenido en un subgrupo maximal M de G y por la hipótesis inductiva obtenemos una serie como (3.2) cuyo último termino es M. Como ya sabemos del Teorema 3.1.4 que $M \lhd G$, la prueba está completa. □

Sea G un grupo y $H \leq G$. Entonces H se llama *característico* si para cualquier automorfismo σ de G, tenemos que $\sigma(H) \subseteq H$, denotaremos esto por $H \text{char} G$. Así tenemos que G y el subgrupo trivial $\{e\}$ son característicos. Ejemplos de subgrupos característicos son el subgrupo derivado $[G, G]$ y el centro $Z(G)$. Sea $g \in G$, un *automorfismo interior* es definido como $T_g(x) = gxg^{-1}$, para cada $x \in G$. Los subgrupos normales son característicos si consideramos solamente los automorfismos interiores, pero no necesariamente si consideramos todos los automorfismos.

Para un grupo finito G, la intersección de sus subgrupos maximales es llamado el *subgrupo de Frattini* de G e es denotado por $\Phi(G)$. Como la imagen de un subgrupo maximal bajo un automorfismo de G es también un subgrupo maximal, $\Phi(G)$ es un subgrupo característico de G. Una razón por la cual este subgrupo tiene un papel importante es el siguiente resultado.

Teorema 3.1.6. *Sea G un grupo finito y sean $x_1, ..., x_m \in G$. Entonces tenemos que $G = \langle x_1, ..., x_n \rangle$ si y solo si $G/\Phi(G) = \langle x_1\Phi(G), ..., x_n\Phi(G) \rangle$.*

Demostración. Es suficiente mostrar la condición necesaria del Teorema. Si $\langle x_1, ..., x_n \rangle$ no es igual a G entonces está contenido en un subgrupo maximal M de G. Así $\langle x_1\Phi(G), ..., x_n\Phi(G) \rangle$ está contenido en $M/\Phi(G)$, que es un subgrupo propio de $G/\Phi(G)$, lo que genera una contradicción. Por tanto necesariamente $G = \langle x_1, ..., x_n \rangle$. □

Teorema 3.1.7. (**El teorema de la base de Burnside**). *Sea G un p-grupo finito. Entonces*

(i) *$G/\Phi(G)$ es un p-grupo abeliano elemental y por tanto puede ser visto como un espacio vectorial sobre $\mathbb{F}_p$.*

(ii) *El conjunto $\{x_1, ..., x_d\}$ es un conjunto mínimo de generadores para G si y solo si $\{x_1\Phi(G), ..., x_d\Phi(G)\}$ es una base para $G/\Phi(G)$.*

(iii) *El mínimo número d de generadores para el grupo G coincide con la dimensión de* $G/\Phi(G)$ *como un* $\mathbb{F}_p$*-espacio vectorial, i.e.* $|G : \Phi(G)| = p^d$.

Demostración. (i) Tenemos que mostrar que $x\Phi(G)y\Phi(G) = y\Phi(G)x\Phi(G)$ y $(x\Phi(G))^p = \Phi(G)$ para todo $x, y \in G$, esto es $x^{-1}y^{-1}xy, x^p \in \Phi(G)$. Por la definición de $\Phi(G)$, es suficiente mostrar que $x^{-1}y^{-1}xy, x^p \in M$ para cualquier subgrupo maximal M de G. Esto es obvio pues de acuerdo con el Teorema 3.1.4, G/M es un grupo de orden p.

(ii) Del teorema anterior tenemos que $S = \{x_1, ..., x_d\}$ es un conjunto de generadores para G si y solo si $\overline{S} = \{x_1\Phi(G), ..., x_d\Phi(G)\}$ es un conjunto de generadores para $G/\Phi(G)$. Por tanto S es un conjunto mínimo de generadores si y solo si $\overline{S}$ lo fuese, que equivale a que $\overline{S}$ sea una base para $G/\Phi(G)$.

(iii) Esto sigue inmediatamente de (ii). □

Si G fuese un grupo finito, denotamos por $d(G)$ el número mínimo de generadores para G.

Definición 3.1.8. Sea G un grupo finito y sea p un primo. Cada subgrupo de G cuyo orden sea la mayor potencia posible de p dividiendo a $|G|$ es llamado un *p-subgrupo de Sylow* de G. Un p-subgrupo de Sylow para algún p es llamado un *p-subgrupo de Sylow*.

En los siguientes teoremas consideraremos que G es un grupo finito y p un número primo dividiendo el orden de G.

Primer teorema de Sylow. *G contiene un p-subgrupo de Sylow y cada p-subgrupo de G está contenido en un p-subgrupo de Sylow de G.*

Segundo teorema de Sylow. *Todos los p-subgrupos de Sylow de G son conjugados.*

Tercer teorema de Sylow. *Sea n_p el número de p-subgrupos de Sylow de G. Escribamos $|G| = p^k m$, donde p no divide a m. Entonces*

$$n_p \equiv 1 \bmod p \quad \text{y} \quad n_p | m.$$

Ahora vamos a ver algunos ejemplos de grupos de automorfismos de p-grupos finitos.

3.2. Automorfismos de grupos finitos

Dado un grupo G, un automorfismo de G es un isomorfismo de G para G, en otras palabras, es un homomorfismo que es al mismo tiempo inyectivo y sobreyectivo. Como el inverso de un automorfismo es un automorfismo y la composición de automorfismos también es un automorfismo, tenemos que el conjunto de todos los automorfismos de G es un grupo. Denotamos este grupo por $Aut(G)$.

Proposición 3.2.1. *Sea G un grupo nilpotente finito, y sea $G = P_1 \times P_2 \times ... \times P_n$, donde P_i son los p-subgrupos de Sylow de G. Entonces*

$$\mathrm{Aut}(G) = \mathrm{Aut}(P_1) \times \mathrm{Aut}(P_2) \times \cdots \times \mathrm{Aut}(P_n).$$

Esta proposición enfoca la atención en la estructura de los p-grupos finitos y los automorfismos de los p-grupos finitos.

Lema 3.2.2. *Sea $g(n)$ el número de grupos de orden n. Entonces*

(i) $g(p) = 1$ *para p primo,*

(ii) *Se $p < q$, entonces $g(pq) = 1$ si $q \not\equiv 1 \bmod p$, y $g(pq) = 2$ en otro caso,*

(iii) $g(p^2) = 2$,

(iv) $g(p^3) = 5$.

A partir de esto, podemos ver que el número de grupos de orden n depende más de la forma de n que de su tamaño. Observemos la siguiente tabla donde comparamos los valores para n y $g(n)$.

n	$g(n)$	n	$g(n)$	n	$g(n)$	n	$g(n)$
1	1	11	1	21	2	31	1
2	1	12	5	22	2	32	51
3	1	13	1	23	1	33	1
4	2	14	2	24	15	34	2
5	1	15	1	25	2	35	1
6	2	16	14	26	2	36	14
7	1	17	1	27	5	37	1
8	5	18	5	28	4	38	2
9	2	19	1	29	1	39	2
10	2	20	5	30	4	40	14

Section 1.3 - David A. Craven, The Theory of p-Groups 2008

El resultado $g(32) = 51$ debe hacer acreditar que, si alguien escoge un grupo G de orden como máximo n al azar, entonces cuando n tiende para el infinito, la probabilidad de que G sea un p-grupo tiende para 1 y, de hecho, G es un 2-grupo no abeliano con probabilidad 1.

Esto junto con los teoremas de Sylow muestran que los p-grupos finitos tienen un papel muy importante en la teoría de grupos finitos.

Proposición 3.2.3. *Sea G un grupo abeliano elemental de orden p^n. Entonces* $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$*, el grupo de $n \times n$ matrices invertibles sobre $\mathbb{F}_p$.*

Demostración. Observe que existen $p^n - 1$ elementos de orden p en G. Supongamos que G es generado por $x_1, ..., x_n$. Un automorfismo del grupo finito es determinado únicamente por su acción en los generadores de un grupo, entonces, si sabemos donde enviar el x_i, podremos crear nuestro automorfismo. Escribimos ϕ para este automorfismo.

También precisamos ver que cualquier elemento de G puede ser expresado como un producto

$$\prod_{i=1}^{n} x_i^{b_i}.$$

donde los b_i son enteros únicos tales que $0 \leq b_i \leq p-1$. Entonces G no puede ser generado por menos de n elementos, en otras palabras no podemos "desperdiciar" un generador atribuyendole para algún lugar que ya podemos expresar en términos de otros generadores. Hablando en términos del álgebra lineal, nos gustaría que las imágenes de los generadores fuesen "linealmente independientes".

Notamos que x_1 puede ser enviado para cualquier elemento de orden p, entonces hay $p^n - 1$ elecciones para $\phi(x_1)$. Ahora tenemos que decidir que hacemos con x_2; no podemos enviarlo para $\langle x_1 \rangle$, ya que estaríamos desperdiciando un generador, y por eso existen $p^n - p$ elecciones para $\phi(x_2)$. Entonces $\langle x_1, x_2 \rangle$ tiene orden p^2, y así existen $p^n - p^2$ elecciones para $\phi(x_3)$, y así en adelante, hasta obtener

$$|\mathrm{Aut}(G)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1}),$$

que es el orden de $\mathrm{GL}_n(\mathbb{F}_p)$. Entonces, si pudiéramos encontrar un homomorfismo de $\mathrm{Aut}(G)$ para $\mathrm{GL}_n(\mathbb{F}_p)$, y mostrar que es inyectivo, habremos terminado.

Usando el hecho que cualquier elemento de G puede ser expresado como un múltiplo de los elementos de la base, procedemos a escribir una matriz para ϕ: sea $A_\phi = (a_{i,j}^{(\phi)})$, donde

$$\phi(x_j) = \sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i.$$

Como A_ϕ es únicamente determinado, tenemos

$$A_\phi(x_1, x_2, ..., x_n) = (\phi(x_1), \phi(x_2), ..., \phi(x_n)).$$

La función $\Phi : \mathrm{Aut}(G) \to \mathrm{GL}_n(p)$ dada por $\phi \mapsto A_\phi$ es inyectiva, como los coeficientes $a_{i,j}^{(\phi)}$ son únicamente determinados. Debemos mostrar que este es un homomorfismo. Si ϕ y ψ son dos elementos de $\mathrm{Aut}(G)$, entonces

$$\begin{aligned}
(\Phi\psi)(\Phi\phi)(x_1) &= \psi(\sum_{i=1}^{n} a_{i,j}^{(\phi)} x_i) \\
&= \sum_{i=1}^{n}\sum_{k=1}^{n} a_{i,j}^{(\phi)} a_{i,j}^{(\psi)} x_k \\
&= \sum_{i=1}^{n}(\sum_{i=1}^{n} a a_{i,j}^{(\phi)} a_{i,j}^{(\psi)}) x_k \\
&= \Phi(\psi\phi)(x_i).
\end{aligned}$$

así $\Phi(\psi\phi) = (\Phi\psi)(\Phi\phi)$ como precisamos. Por tanto $\mathrm{Aut}(G) \cong \mathrm{GL}_n(\mathbb{F}_p)$. □

Proposición 3.2.4. *Sea G un grupo cíclico de orden n. Entonces el $\mathrm{Aut}(G)$ es abeliano y tiene orden $\phi(n)$, donde ϕ denota la función ϕ de Euler.*

Demostración. Sea $G = \langle x \rangle$. Entonces un automorfismo G debe enviar x para otro generador de G, el que obviamente debe tener orden n, y así se reduce a descubrir cuantos elementos de C_n tienen orden n. Si n y m son coprimos, con $1 \leq m \leq n$, entonces el primer entero k para el cual $x^{mk} = 1$ es $k = n$. Por tanto, si m y n son coprimos entonces x^m tiene orden n. En otro lado, sea d el $\mathrm{mcd}(m, n)$ y supongamos que x^m tiene orden n. Como

$(x^m)^{n/d} = 1$ (pues mn/d es divisible por n), $n \leq n/d$; esto claramente implica que $d = 1$ y así m y n son coprimos.

Hemos probado que x^m tiene orden n si y solo si m y n son coprimos, y por tanto $|\mathrm{Aut}(G)| = \phi(n)$, pues la función ϕ de Euler es simplemente la cantidad de números $m \leq n$ coprimos con n.

Para ver que $\mathrm{Aut}(G)$ es abeliano, observemos que todos los automorfismos tienen la forma $x \mapsto x^m$; si $\phi : x \mapsto x^m$ y $\psi : x \mapsto x^k$ son dos automorfismos, entonces

$$(\psi\phi)x = \psi(\phi x) = \psi x^m = x^{mk} = \phi x^k = (\phi\psi)x.$$

y así $\mathrm{Aut}(G)$ es abeliano. □

Podemos mejorar la proposición anterior en el caso en que el grupo cíclico es de orden primo.

Proposición 3.2.5. *Sea $G \cong C_p = \langle x \rangle$. Entonces $\mathrm{Aut}(G)$ es cíclico de orden $p - 1$.*

Demostración. Ya sabemos que $\mathrm{Aut}(G)$ es abeliano de orden $p - 1$ (pues cualquier número menor que p es coprimo con p), entonces solamente precisamos mostrar que $\mathrm{Aut}(G)$ es cíclico. Para ver eso, observemos que $\mathrm{Aut}(G)$ es lo mismo que multiplicar los enteros diferentes de cero módulo p. Entonces como los enteros módulo un primo forman un cuerpo, $\mathrm{Aut}(G)$ es cíclico.

Consideremos dos automorfismos $\phi_m : x \mapsto x^m$ y $\phi_k : x \mapsto x^k$, donde m y k están entre 1 y $p - 1$. Entonces $\phi_m\phi_k$ es dado por

$$\phi_{mk} : x \mapsto x^{mk}.$$

entonces obtenemos un homomorfismo de $\mathrm{Aut}(G)$ para el grupo multiplicativo de enteros módulo p por

$$\Phi : \mathrm{Aut}(G) \to (\mathbb{Z}/p\mathbb{Z})^*, \qquad \Phi : \phi_m \mapsto m.$$

(Donde, $F^* = F\backslash\{0\}$ denota el subgrupo multiplicativo de F). Por tanto $\mathrm{Aut}(G)$ es cíclico de orden $p - 1$, como queríamos. □

Observe que en este caso $|G| > |\mathrm{Aut}(G)|$ entonces $|G| \nmid |\mathrm{Aut}(G)|$. En general en la mayoría de los casos de p-grupos finitos, $|G|$ divide a $|\mathrm{Aut}(G)|$.

J. González-Sánchez y A. Jaikin-Zapirain en su trabajo mencionan lo siguiente (2015):

Una pregunta bien conocida (ver, por ejemplo, [Mazurov, 2010]) nos dice si es verdad que $|G|$ divide a $|\mathrm{Aut}(G)|$ para cada p-grupo finito no-abeliano G. No está claro quién formuló la pregunta por primera vez; el primer resultado en ese sentido que encontramos en la literatura es debido a Schenkman (1955), que fue publicado hace mas de 60 años. En ese artículo, Schenkman mostró que eso es verdad para p-grupos finitos no abelianos de clase 2 (la prueba tiene un error que fue corregido por Faudree en (1968)). Mas tarde, también fue establecido para p-grupos de exponente p en (R. Ree, 1958), para p-grupos de clase maximal en (Otto, 1966), para p-grupos con centro de orden p en (Gazchütz, 1965), para p grupos metacíclicos cuando p es impar en (Davitt, 1970), para p-grupos

central-metacíclicos cuando p es impar en (Davitt, 1971), para p-grupos p-abelianos en (Davitt, 1972) (vea también (Thillaisundaram, 2012)), para p-grupos modulares finitos en (Davitt, 1972), para algunos productos centrales en (Buckey, 1975/1976; Hummel, 1975), para p-grupos con centro de índice como máximo p^4 en (Davitt, 1980), para p-grupos con subgrupo de Frattini cíclico en (Exarchakos, 1981), para p-grupos de orden como máximo p^6 en (David, 1980; Exarchakos, 1989), para p-grupos de orden como máximo p^7 en (Gavioli, 1993), para p-grupos de coclase 2 en (Fouladi, 2007) (vea también un resultado relacionado en (Eick, 2006)), y para p-grupos G tales que $(G, Z(G))$ es una "Camina pair" en (Yadav, 2007).

Todos esos resultados parciales muestran la dificultad de obtener un contra-ejemplo. El trabajo realizado por J. González-Sánchez. y A. Jaikin-Zapirain (29) utiliza técnicas pro-p, y el objetivo es mostrar el siguiente Teorema (Para mayores detalles sobre la prueba ver Capítulo 9).

Teorema principal. *Para cada primo p existe una familia de p-grupos finitos $\{U_i\}$ tal que*

$$\lim_{i\to\infty} |U_i| = \infty \qquad \text{e} \qquad \limsup_{i\to\infty} \frac{|\mathrm{Aut}U_i|}{|U_i|^{40/41}} < \infty.$$

En particular, para cada primo p, existe un p-grupo finito no abeliano tal que $|\mathrm{Aut}(G)| < |G|$.

La construcción realizada por González y Jaikin consiste de dos partes; que ellos describen así:

(i) **Primera parte.** Vamos a considerar un grupo pro-p infinito finitamente U generado tal que $\dim(\mathrm{Aut}(U)) < \dim(U)$, donde $\dim\ U$ es definida como $\dim_{\mathbb{Q}_p}\mathbf{L}(U)$, donde $\mathbf{L}(U)$ es una $\mathbb{Q}_p$-álgebra de Lie asociada a U. Podemos hacer esto pues U es un grupo pro-p analítico p-ádico y por tanto $\mathrm{Aut}(U)$ es un grupo profinito analítico p-ádico.

(ii) **Segunda parte.** Escribamos U como un límite inverso de la familia de p-grupos finitos $\{U_i\}$ donde $U_i = U/U^{p^i}$. Así $U = \varprojlim U_i$, y por eso $\mathrm{Aut}U_i = \varprojlim \mathrm{Aut}U_i$, de donde esperamos que para algún i podamos tener $|\mathrm{Aut}(U_i)| < |U_i|$. (Gonzáles-Jaikin, 2015).

Para tener una idea sobre la primera parte: puesto que U es un grupo pro-p uniforme, tenemos que

$$\dim\ \mathrm{Aut}(U) = \dim_{\mathbb{Q}_p}\mathrm{Der}\mathbf{L}(U),$$

donde $\mathrm{Der}\mathbf{L}(U)$ es una $\mathbb{Q}_p$-álgebra de derivaciones internas de $\mathbf{L}(U)$. Un ejemplo de álgebras de Lie L con $\dim\ \mathrm{Der}(L) < \dim\ L$ es construida por Sato (Sato, 1971) y vamos a discutir eso en el capítulo 7 de este trabajo; esta álgebra es construida sobre $\mathbb{Q}$ y tiene dimensión 41 con centro de dimensión 1, así el álgebra consiste solamente de derivaciones internas y por tanto tiene dimensión 40.

La segunda parte está basada en el análisis de la primera cohomología de grupos $H^1(U, L_i)$, donde $L_i = \mathbf{log}(U)/p^i\mathbf{log}(U)$ y $\mathbf{log}(U)$ es el anillo de Lie correspondiente al grupo pro-p uniforme U por la correspondencia de Lazard. Tenemos que $\mathrm{Der}(\mathbf{L}(U)) = \mathrm{Inn}(\mathbf{L}(U))$; sigue que $\mathrm{Der}(\mathbf{log}(U))$ es finito y por tanto

$$H^1_{cts}(U, \mathbf{log}(U)) \cong \mathrm{Der}(\mathbf{log}(U))$$

es también finito. Esto implica la existencia de una cota superior para $|H^1(U, L_i)|$. Ahora, si definimos $U_i = U/U^{p^i}$ tendríamos una cota superior para $|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)|$ y culminamos con la prueba.

Capítulo 4

Grupos nilpotentes

En este capítulo desarrollamos la teoría clásica de grupos nilpotentes. Incluyendo resultados conocidos y algunos novedosos. El libro que nos servirá de guía para esta sección es "The Theory of Nilpotent Groups" (Clement, 2017, pp: 23-50).

4.1. Cálculo del conmutador

Una de las herramientas más importantes en el estudio de los grupos nilpotentes es el cálculo del conmutador. Definiremos el centro de un grupo y otras nociones de conmutatividad. El conmutador de dos elementos g, h en un grupo dado G está definido por $[g, h] = g^{-1}h^{-1}gh$. De aquí, claramente $[g, h] = 1$ si y solo si g y h conmutan.

Definición 4.1.1. Sea G un grupo, y sean g, h en G. El *conjugado* de g por h será el elemento g^h de G definido por

$$g^h = h^{-1}gh.$$

Lema 4.1.2. *Sea G un grupo, y sean g, h y k en G. Entonces $(gh)^k = g^k h^k$, $(g^{-1})^h = (g^h)^{-1}$ y $(g^h)^k = g^{hk}$*

Demostración.
Por definición tenemos $(gh)^k = k^{-1}(gh)k = k^{-1}g(kk^{-1})hk = (k^{-1}gk)(k^{-1}hk) = g^k h^k$. Las otras dos son análogas. □

Definición 4.1.3. Sea G un grupo, y sean H y K subgrupos de G. Diremos que H y K son *conjugados* si

$$g^{-1}Hg = K, \qquad \text{para algún } g \in G.$$

De esta manera, un subgrupos normal sería conjugado de si mismo.

Definición 4.1.4. Sea G un grupo y sea g un elemento de G. Llamaremos a g *central* si conmuta con cada elemento de G. El conjunto de todos los elementos centrales del grupo G se llamará el *centro* de G y será denotado por $Z(G)$. Así

$$\begin{aligned} Z(G) &= \{g \in G \mid gh = hg, \text{ para todo } h \in G\} \\ &= \{g \in G \mid g^h = g, \text{ para todo } h \in G\} \end{aligned}$$

No es difícil ver que $Z(G)$ es un subgrupo normal de G, y que cada elemento de $Z(G)$ es conjugado de si mismo.

Lema 4.1.5. *Sean G_1 y G_2 dos grupos. Entonces $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.*

Lema 4.1.6. *Sean G_1 y G_2 dos grupos. Entonces*

$$\frac{G_1 \times G_2}{Z(G_1 \times G_2)} \cong \frac{G_1}{Z(G_1)} \times \frac{G_2}{Z(G_2)}.$$

Definición 4.1.7. Sea G un grupo y sea h en G. El mapeo $\varphi_h : G \to G$ definido por $\varphi_h(g) = g^h$ es un automorfismo de G ($\varphi_h \in \mathrm{Aut}(G)$) y lo llamaremos *mapeo conjugado* o *automorfismo interno*. El conjunto de todos los automorfismos internos es un subgrupo de $\mathrm{Aut}(G)$ y será denotado por $\mathrm{Inn}(G)$.

Teorema 4.1.8. *Sea G un grupo y sea h en G. El mapeo*

$$\begin{aligned} \varrho : G &\to \mathrm{Aut}(G) \\ h &\mapsto \varphi_h \end{aligned}$$

donde $\varphi_h(g) = g^h$, es un homomorfismo con $ker\varrho = Z(G)$ e $im\varrho = \mathrm{Inn}(G)$.

Corolario 4.1.9. *Sea G un grupo, entonces*

$$\frac{G}{Z(G)} \cong \mathrm{Inn}(G).$$

Ejemplo 4.1.10. Un grupo G es abeliano si y solo si $Z(G) = G$.

Ejemplo 4.1.11. Sea S_n el grupo simétrico sobre el conjunto $S = \{1, 2, \cdots, n\}$ y denotemos el elemento identidad de S_n con $\{e\}$. Así, S_1 tiene centro trivial pues $S_1 = \{e\}$, $Z(S_2) = S_2$ pues S_2 es abeliano y tenemos que $Z(S_n) = \{e\}$, para $n > 2$. Para el grupo alternante tenemos que $Z(A_n) = A_n$, para $n = 1, 2$ o 3.

Ejemplo 4.1.12. Sea $\mathscr{H}$ el grupo de matrices triangulares superiores 3×3 sobre $\mathbb{Z}$, donde la operación del grupo es la multiplicación de matrices. Así,

$$\mathscr{H} = \left\{ \begin{pmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a_{ij} \in \mathbb{Z} \right\}$$

Este grupo es llamado el *Grupo de Heisenberg*. El elemento identidad en $\mathscr{H}$ es claramente la matriz identidad 3x3, la cual es denotada por I_3. No es difícil probar que

$$Z(\mathscr{H}) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, c \in \mathbb{Z} \right\}.$$

Definición 4.1.13. Un subgrupo H de un grupo G es llamado *central* si $H \leq Z(G)$.

Definición 4.1.14. Sea G un grupo y X un subconjunto no vacío de G. El *centralizador* de X en G, será

$$C_G(X) = \{g \in G \mid g^{-1}xg = x \text{ para todo } x \in X\}$$

No es difícil probar que $C_G(X) \leq G$ y que $C_G(G) = \cap_{X \subseteq G} C_G(X) = Z(G)$. Si $X = \{x\}$, entonces podemos escribir $C_G(x)$ para el centralizador de x.
Si G es finito, tenemos la *ecuación de clases* de G:

$$|G| = |Z(G)| + \sum_k [G : C_G(x_k)],$$

donde la clase de conjugación de cada x_k contiene al menos dos elementos.

Definición 4.1.15. Sea G un grupo y sean g, h en G. El conmutador de g y h es

$$[g, h] = g^{-1}h^{-1}gh = g^{-1}g^h.$$

Claramente, g y h conmuta si y solo si $[g, h] = 1$. Así, podemos escribir el centro de G como

$$Z(G) = \{g \in G \mid [g, h] = 1, \text{ para todo } h \in G\}.$$

Definición 4.1.16. Sea $S = \{g_1, g_2, \cdots, g_n\}$ un subconjunto de un grupo G. El *conmutador simple* o *conmutador a la izquierda*, de *peso* $n \geq 1$ es definido recursivamente como:

1. Conmutador simple de peso 1 son todos los elementos de S, escribimos $g_j = [g_j]$,
2. Conmutador de peso $n > 1$ son $[g_1, \cdots, g_n] = [[g_1, \cdots, g_{n-1}], g_n]$.

Enseguida algunas propiedades del conmutador.

Lema 4.1.17. *Sea G un grupo y sean x, y y z elementos de G.*

(i) $xy = yx[x, y]$

(ii) $x^y = x[x, y]$

(iii) $[x, y] = [y, x]^{-1}$

(iv) $[x, y]^z = [x^z, y^z]$

(v) $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$

(vi) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$

(vii) $[x.y^{-1}] = ([x, y]^{y^{-1}})^{-1}$

(viii) $[x^{-1}, y] = ([x, y]^{x^{-1}})^{-1}$

Demostración.

(i) $xy = 1.xy = (yxx^{-1}y^{-1})xy = yx[x, y]$

(ii) $x^y = y^{-1}xy = x(x^{-1}y^{-1}xy) = x[x, y]$

(iii) $[x,y] = x^{-1}y^{-1}xy = (y^{-1}x^{-1}yx)^{-1} = [y,x]^{-1}$

(iv) $[x,y]^z = z^{-1}[x,y]z = z^{-1}(x^{-1}y^{-1}xy)z = (z^{-1}x^{-1}z)(z^{-1}y^{-1}z)(z^{-1}xz)(z^{-1}yz) = (x^z)^{-1}(y^z)^{-1}x^zy^z = [x^z,y^z]$

(v) $[xy,z] = (xy)^{-1}z^{-1}(xy)z = (y^{-1}x^{-1}z^{-1}xzy)(y^{-1}z^{-1}yz) = [x,z]^y[y,z] =$
$= ([x,z][x,z,y])[y,z]$ (por (ii))

(vi) Análogo a (v)

(vii) $1 = [x,yy^{-1}] = [x,y^{-1}][x,y]^{y^{-1}}$ (por (vi))

(viii) Análogo a (vii). □

Lema 4.1.18. (Las identidades de Hall-Witt). *Sea G un grupo, y sean x, y y z elementos de G, entonces*

$$[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$$

y

$$[x,y,z^x][z,x,y^z][y,z,x^y] = 1$$

Demostración.

$$\begin{aligned}
[x,y^{-1},z]^y &= y^{-1}[x.y^{-1},z]y \\
&= y^{-1}[[x,y^{-1}],z]y \\
&= y^{-1}[x,y^{-1}]^{-1}z^{-1}[x,y^{-1}]zy \\
&= y^{-1}[y^{-1},x]z^{-1}[x,y^{-1}]zy \qquad \text{(por el Lema 4,1,17.}(iii)\text{)} \\
&= y^{-1}(yx^{-1}y^{-1}x)z^{-1}(x^{-1}yxy^{-1})zy \\
&= (xzx^{-1}yx)^{-1}(yxy^{-1}zy)
\end{aligned}$$

los otros dos conmutadores son análogos

- $[y,z^{-1},x]^z = (yxy^{-1}zy)^{-1}(zyz^{-1}xz)$,
- $[z,x^{-1},y]^x = (zyz^{-1}xz)^{-1}(xzx^{-1}yx)$

Así, finalmente tenemos que

$$[x,y^{-1},z]^y[y,z^{-1},x]^z[z,x^{-1},y]^x = 1$$

La otra identidad es muy similar. □

4.2. Subgrupo conmutador

Generalicemos la noción de conmutador de un elemento de un grupo a la de un subgrupo dentro de un grupo dado.

Definición 4.2.1. Sea G un grupo y sea $S = \{s_1, s_2, \cdots\}$ un subconjunto de G. El subgrupo de G *generado* por S, denotado por

$$gp(S) = gp(s_1, s_2, \cdots),$$

es el menor subgrupo de G que contiene a S. Llamaremos a S el conjunto de *generadores* para $gp(S)$. Los elementos de $gp(S)$ tienen la forma

$$s_{i1}^{e_1} s_{i2}^{e_2} \cdots s_{in}^{e_n}$$

donde los $s_{ij} \in S$ y $e_j \in \{-1, 1\}$, con $1 \leq j \leq n$. Así, $gp(g)$ es el subgrupo cíclico de G generado por g. Si $S_1, S_2, \cdots, S_n$ son subconjuntos de G, entonces el subgrupo $gp(S_1 \cup \cdots \cup S_n)$ es escrito como $gp(S_1, \cdots, S_n)$.

Definición 4.2.2. Sea G un grupo y sean X_1, X_2 subconjuntos no vacios de G. El *subgrupo conmutador* de X_1 y X_2 es definido como

$$[X_1, X_2] = sp([x_1, x_2] \mid x_1 \in X_1, x_2 \in X_2).$$

En particular, al subgrupo $G' = [G, G]$ se le llamará *subgrupo conmutador* o *subgrupo derivado* de G.

Definición 4.2.3. Sea $\{X_1, X_2, \cdots\}$ una colección de subconjuntos de un grupo G, entonces

$$[X_1, \cdots, X_n] = [[X_1, \cdots, X_{n-1}], X_n],$$

donde $n \geq 2$.

Lema 4.2.4. *Sea G un grupo.*

(i) *Si $H \leq G$ y $[G, G] \leq H$, entonces $H \lhd G$ y G/H es abeliano. En particular, $[G, G] \lhd G$ y $G/[G, G]$ es abeliano.*

(ii) *Si $N \lhd G$ y G/N es abeliano, entonces $[G, G] \lhd N$.*

Así, el subgrupo derivado $[G, G]$ es el menor subgrupo normal induciendo un cociente abeliano. El grupo cociente $Ab(G) = G/[G, G]$ es llamado la *abelianización* de G.

Demostración.
(i) Sea $h \in H$ y $g \in G$, entonces $g^{-1}hg = h(h^{-1}g^{-1}hg) = h[h, g] \in H[G, G] = H$ (Por hipótesis), así $H \lhd G$. Sean g_1H y g_2H en G/H, entonces $g_1g_2H = g_2g_1[g_1, g_2]H = g_2g_1H$. Por tanto, G/H es abeliano.
(ii) Sean g_1, g_2 en G, entonces $g_1g_2N = g_2g_1N$ (pues N es normal en G), entonces $[g_1, g_2]N = N$ y por tanto $[g_1, g_2] \in N$. Por ende, $[G, G] \leq N$. Por otro lado, $h^{-1}[g_1.g_2]h = [g_1, g_2][g_1, g_2]^{-1}h^{-1}[g_1, g_2]h$. Concluimos que $[G, G] \lhd N$. □

Ejemplo 4.2.5. Sea G un grupo abeliano, entonces $[G, G] = 1$.

Ejemplo 4.2.6. Sea S_n el grupo simétrico de orden n, entonces $[S_n, S_n] = \{e\}$, para $n = 1, 2$ y $[S_n, S_n] = A_n$, para $n \geq 3$.

Ejemplo 4.2.7. Mostraremos que el subgrupo derivado del grupo de Heisenberg $\mathscr{H}$ es igual a su centro. Por el Ejemplo 4.1.12, el centro de $\mathscr{H}$ es

$$Z(\mathscr{H}) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, c \in \mathbb{Z} \right\} = gp\left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right)$$

Sean

$$a = \begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 1 & a_3 \\ 0 & 0 & 1 \end{pmatrix} \quad y \quad b = \begin{pmatrix} 1 & b_1 & b_2 \\ 0 & 1 & b_3 \\ 0 & 0 & 1 \end{pmatrix}$$

elementos de $\mathscr{H}$, entonces

$$[a, b] = \begin{pmatrix} 1 & 0 & a_1b_3 - b_1a_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Así, $[\mathscr{H}, \mathscr{H}] \leq Z(\mathscr{H})$. Además

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right]$$

sigue que $Z(\mathscr{H}) \leq [\mathscr{H}, \mathscr{H}]$. Por tanto tenemos que

$$[\mathscr{H}, \mathscr{H}] = Z(\mathscr{H}).$$

Definición 4.2.8. Sea G un grupo y sean $H \leq G$ y $A \subseteq \mathrm{Aut}(G)$ un subconjunto del grupo de automorfismos de G.

(i) Si para cada $\varphi \in A$ y $h \in H$, tenemos que $\varphi(h) \in H$, entonces H se llama A-invariante.

(ii) Si H es $\mathrm{Aut}(G)$-invariante, entonces H es llamado *característico* en G.

(iii) Si cada endomorfismo de G se puede restringir a un endomorfismo de H, entonces H se llama *completamente invariante*.

Lema 4.2.9. *Sea G un grupo. Si H es un subgrupo característico de G, entonces $H \lhd G$.*

Lema 4.2.10. (P. Hall). *Sea G un grupo y sean H y K subgrupos de G, supongamos que $[H.K] \leq Z(G)$. Si $a \in H$ y $b \in K$, entonces las siguientes aplicaciones*

$$\begin{array}{ccc} \varphi_a : K \to Z(G) & \text{y} & \varphi_b : H \to Z(G) \\ k \mapsto [a, k] & & h \mapsto [h, b] \end{array}$$

son homomorfismos.

Demostración. Sean $k_1, k_2 \in K$. Entonces

$$[a, k_1k_2] = [a, k_2][a, k_1]^{k_2} = [a, k_2][a, k_1] \qquad \text{(Lema 4,1,17.}(vi)\text{)}$$

Por tanto, φ_a es homomorfismo. Del mismo modo, tenemos que φ_b es también homomorfismo. □

Lema 4.2.11. *Sea G un grupo. Si $[g, h] \in Z(G)$ para algunos $g, h \in G$ y $n \in \mathbb{Z}$. Entonces*

$$[g^n, h] = [g, h]^n = [g, h^n].$$

4.3. Series central, inferior y superior

Antes de definir un grupo nilpotente, nos vemos en la necesidad de definir lo que significa una Serie Central Inferior y Superior.

Definición 4.3.1. Sea G un grupo. Una *serie* para G es una cadena finita de subgrupos de la forma

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G \tag{4.1}$$

En el caso que todos los subgrupos sean diferentes, n es llamada la *longitud* de la serie. Se dirá que la serie es *normal* si $G_i \lhd G$, para todo $0 \leq i \leq n$, y *subnormal* si $G_i \lhd G_{i+1}$, para $0 \leq i \leq n-1$. Los factores de una serie subnormal son los cocientes G_{i+1}/G_i, para $0 \leq i \leq n-1$.

Cada serie normal es subnormal, pero la inversa no siempre es cierta. Un claro ejemplo de esto es el grupo simétrico de orden 4, S_4. Sea $G_1 = \{e, (1\,2)(3\,4)\}$ y $G_2 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$. Así, la serie de grupos

$$\{e\} \lhd G_1 \lhd G_2 \lhd A_4 \lhd S_4$$

es subnormal, mas no es normal, pues G_1 no es normal en S_4

$$(1\,2\,3\,4)^{-1}(1\,2)(3\,4)(1\,2\,3\,4) \notin G_1.$$

Definición 4.3.2. Sea G un grupo y sea $S = \{G_1, G_2, G_3, \cdots\}$ una sucesión de subgrupos de G.

(i) Si $G_i \leq G_j$, para $1 \leq i \leq j$, entonces

$$G_1 \leq G_2 \leq G_3 \leq \cdots$$

es una *serie ascendente* (o una *cadena ascendente de subgrupos* en G.)

(i) Si $G_i \geq G_j$, para $1 \leq i \leq j$, entonces

$$G_1 \geq G_2 \geq G_3 \geq \cdots$$

es una *serie descendente* (o una *cadena descendente de subgrupos en* G.)

Definición 4.3.3. Un grupo G es llamado *nilpotente* si posee una serie normal

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G \tag{4.2}$$

tal que

$$G_{i+1}/G_i \leq Z(G/G_i)$$

para $i = 0, 1, \cdots, n-1$. La serie en (4.2) se llamará *serie central* para G. La menor longitud de todas las series para G es llamada la *clase de nilpotencia*, o simplemente la *clase*, de G.

Lema 4.3.4. *Sea G un grupo y sea la serie*

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G. \tag{4.3}$$

La serie (4.3) es central si y solo si $[G_{i+1}, G] \leq G_i$, para $0 \leq i \leq n-1$.

Lema 4.3.5. *Si G es un grupo nilpotente no trivial, entonces $Z(G) \neq 1$.*

Demostración. Supongamos que $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ es una serie central para G. Debe existir un entero $i \geq 0$ tal que $G_i = 1$ y $G_{i+1} \neq 1$. Por hipótesis tenemos que, $G_{i+1}/G_i \leq Z(G/G_i)$. Sea $a \in G_{i+1}$, entonces $aG_i \in Z(G/G_i)$, tomemos un $b \in G$, tenemos que $abG_i = baG_i$, esto implica que $[a, b] \in G_i$, para todo $b \in G$. Entonces $[a, b] = 1$. Así, $a \in Z(G)$. Por tanto, $G_{i+1} \leq Z(G)$. Sigue que $Z(G) \neq 1$. □

Definición 4.3.6. Un grupo G se llama *soluble* si tiene una serie subnormal.

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

tal que G_{i+1}/G_i es abeliano para $0 \leq i \leq n-1$. Entonces cada grupo nilpotente es soluble, pero lo contrario no siempre es cierto. Un ejemplo de ello es el grupo simétrico de orden 3, S_3. Tenemos la serie subnormal $1 \lhd A_3 \lhd S_3$ de factores abelianos, sin embargo $Z(S_3) = 1$. Por tanto, por el Lema 4.3.5 S_3 no puede ser nilpotente.

Definición 4.3.7. Sea G un grupo. La serie descendente

$$G = \gamma_1 G \geq \gamma_2 G \geq \cdots \tag{4.4}$$

definida recursivamente por $\gamma_{i+1}G = [\gamma_i G, G]$ para $i \in \mathbb{N}$ es llamada la *serie central inferior* de G y sus términos serán llamados *subgrupos centrales inferiores* de G.

El subgrupo derivado de G será $\gamma_2 G = [G, G] = G'$. Por definición tenemos que

$$\gamma_i G = \underbrace{[G, \cdots, G]}_{i}$$

para $i \geq 2$. Se define que $\gamma_i G \lhd G$, para $i \geq 1$.

Ejemplo 4.3.8. Si G es un grupo abeliano, entonces $[G, G] = 1$. Así, $\gamma_i G = 1$, para todo $i \geq 2$.

Ejemplo 4.3.9. Sea S_n el grupo simétrico sobre el conjunto $S = \{1, 2, \cdots, n\}$. Tenemos que $\gamma_i S_1 = \gamma_i S_2 = \{e\}$, para $i \geq 2$. Consideremos $n = 3$. Se demuestra que $[S_3, S_3] = A_3$ y $[(a\ c\ b), (a\ b)] = (a\ c\ b)$ para distintos $a, b, c \in S$, sigue que $\gamma_3 S_3 = [\gamma_2 S_3, S_3] = [A_3, S_3] = A_3$. Así, tenemos que $\gamma_i S_3 = A_3$, para $i \geq 2$. Ahora, consideremos $n = 4$. Sabemos que $A_4 \leq [S_4, A_4]$. Además $[S_4, A_4] \leq [S_4, S_4] = A_4 \leq [S_4, A_4]$. Entonces $A_4 = [S_4, A_4]$. Por tanto, $\gamma_3 S_4 = A_4$, así $\gamma_i S_4 = A_4$, para $i \geq 2$. Ahora que pasa si $n \geq 5$. $[S_n, S_n] = A_n$ y $A_n = [A_n, A_n]$, para $n \geq 5$. por tanto $A_n = [A_n, A_n] \leq [S_n, A_n] \leq [S_n, S_n] = A_n$. Así, $\gamma_3 S_n = [S_n, A_n] = A_n$, luego $\gamma_i S_n = A_n$, $i \geq 2$.

Ejemplo 4.3 10. Sabemos que el grupo de Heisenberg cumple que $[\mathscr{H}, \mathscr{H}] = Z(\mathscr{H})$, lo que significa que $\gamma_2 \mathscr{H} = Z(\mathscr{H})$. Así

$$\gamma_3 \mathscr{H} = [Z(\mathscr{H}), \mathscr{H}] = I_3$$

luego, $\gamma_i\mathscr{H} = I_3$, para todo $i \geq 3$. Por tanto la serie central inferior de $\mathscr{H}$ es central en el sentido de la Definición 4.3.3. Finalmente, $\mathscr{H}$ es nilpotente.

Lema 4.3.11. *Los subgrupos centrales inferiores de un grupo son totalmente invariantes (por tanto, característicos).*

Lema 4.3.12. *Sea G un grupo y $H \leq G$, entonces*

$$\gamma_i H \leq \gamma_i G, \text{ para cada } i \in \mathbb{N}.$$

Demostración. Probaremos esto por inducción sobre i. Si $i = 1$, es cierto. Supongamos que $\gamma_i H \leq \gamma_i G$ para $i > 1$. Entonces

$$\gamma_{i+1}H = [\gamma_i H, H] \leq [\gamma_i G, G] = \gamma_{i+1}G. \ \square$$

Lema 4.3.13. *Sean G y K dos grupos $\varphi : G \to K$* es un homomorfismo, entonces $\varphi(\gamma_i G) = \gamma_i(\varphi G)$, para cada $i \in \mathbb{N}$. Así tenemos que $\varphi(\gamma_i G) \leq \gamma_i K$. La igualdad se da cuando φ es suryectiva.

Corolario 4.3.14. Sea G un grupo y sea $N \lhd G$, entonces $\gamma_i(G/N) = (\gamma_i G)N/N$, para todo $i \in \mathbb{N}$.

Lema 4.3.15. *Sea G un grupo. Para cada $n \in \mathbb{N}$, tenemos*

$$\gamma_n G = gp([g_1, \cdots, g_n] \mid g_i \in G).$$

Además, si X genera G, entonces $g_n G$ es generado por todos los conmutadores de peso n o más en los elementos de X y sus inversos.

Sea G un grupo. Sea $\zeta_1 G = Z(G)$ y $\pi_1 : G \to G/\zeta_1 G$ el homomorfismo natural de paso al cociente. Definamos

$$\zeta_2 G = \pi_1^{-1}(Z(G/\zeta_1 G))$$

Así, $\zeta_2 G/\zeta_1 G = Z(G/\zeta_1 G)$ y por el Teorema de la Correspondencia $\zeta_2 G \lhd G$.

Sea $\pi_2 : G \to G/\zeta_2 G$ el homomorfismo natural de paso al cociente, definamos

$$\zeta_3 G = \pi_2^{-1}(Z(G/\zeta_2 G))$$

Así, $\zeta_3 G/\zeta_2 G = Z(G/\zeta_2 G)$. También $\zeta_3 G \lhd G$. Siguiendo con este proceso recursivamente definimos los subgrupos de la serie central superior de G.

Definición 4.3.16. Sea G un grupo. La serie ascendente

$$1 = \zeta_0 G \leq \zeta_1 G \leq \cdots \tag{4.5}$$

definida recursivamente por $\zeta_{i+1}G/\zeta_i G = Z(G/\zeta_i G)$, para $i \geq 0$ es llamada la *serie central superior* de G, y sus términos son llamados los *subgrupos centrales superiores* de G.

Si $\pi_i : G \to G/\zeta_i G$ es el homomorfismo natural de G para $G/\zeta_i G$, entonces

$$\begin{aligned}\zeta_{i+1}G &= \pi^{-1}(Z(G/\zeta_i G)) \\ &= \{g \in G \mid g\zeta_i G \text{ es central en } G/\zeta_i G\} \\ &= \{g \in G \mid (g\zeta_i G)(h\zeta_i G) = (h\zeta_i G)(g\zeta_i G) \text{ para todo } h \in G\} \\ &= \{g \in G \mid [g,h] \in \zeta_i G \text{ para todo } h \in G\}\end{aligned}$$

En particular, $\zeta_1 G$ es el centro de G. Tomando $N = \zeta_i G$ y $H = \zeta_{i+1}G$, tenemos que $[\zeta_{i+1}G, G] \leq \zeta_i G$.

Observación 4.3.17. Sea G un grupo.

(i) Si $\zeta_i G = G$ para algún $i \geq 0$, entonces $\zeta_j G = G$, para $j \geq i$. Así, una serie central superior es también una serie central en el sentido de la Definición 4.3.3.

(ii) Si $Z(G) = 1$, entonces $\zeta_j G = 1$, para $j \geq 0$.

Ejemplo 4.3.18. Si G es un grupo abeliano, entonces $\zeta_1 G = G$. Entonces $\zeta_i G = G$, para $i \geq 1$ (Observación 4.3.17 (i)).

Ejemplo 4.3.19. Si $n \geq 3$, la serie central superior de S_n es trivial (Ejemplo 4.1.11 y Observación 4.3.17 (ii)). Lo mismo acontece para la serie central superior de A_n cuando $n > 3$. Esto nos dice que la serie central superior de un grupo no necesariamente asciende al grupo.

Ejemplo 4.3.20. Sea $\mathscr{H}$ el grupo de Heinsenberg. Por el ejemplo 4.2.7 $Z(\mathscr{H} = [\mathscr{H}, \mathscr{H}])$. Así

$$\zeta_2\mathscr{H} = \{g \in \mathscr{H} \mid [g,h] \in Z(\mathscr{H}) \text{ para todo } h \in \mathscr{H}\} = \mathscr{H}$$

Por tanto $\zeta_i\mathscr{H} = \mathscr{H}$ para $i \geq 2$ (Observación 4.3.17 (i)). Por otro lado, $\gamma_1\mathscr{H} = \mathscr{H}$. Entonces $\gamma_1\mathscr{H} = \zeta_2\mathscr{H}$, $\gamma_2\mathscr{H} = \zeta_1\mathscr{H}$ y $\gamma_3\mathscr{H} = I_3 = \zeta_0\mathscr{H}$. Así, las series central inferior y superior de $\mathscr{H}$ coinciden.

Lema 4.3.21. *Sean G y H dos grupos y sea $\varphi : G \to H$ un epimorfismo, entonces $\varphi(\zeta_i G) \leq \zeta_i H$, para $i \geq 0$.*

Corolario 4.3.22. *Los subgrupos centrales superiores de un grupo son característicos.*

Teorema 4.3.23. *Si G es un grupo nilpotente con serie central (descendente)*

$$G = G_1 \geq G_2 \geq \cdots \geq G_n \geq G_{n+1} = 1$$

entonces $\gamma_i G \leq G_i$ y $G_{n-j+1} \leq \zeta_j G$ para $1 \leq i \leq n+1$ y $0 \leq j \leq n$.

Corolario 4.3.24. *Sea G un grupo. Las siguientes son equivalentes:*

(i) *G es nilpotente de clase a lo más c*

(ii) $\gamma_{c+1}G = 1$

(iii) $\zeta_c G = G$

(iv) $[g_1, \cdots, g_{c+1}] = 1$, *para todo* $g_i \in G$.

Teorema 4.3.25. *Sea G un grupo. Las siguientes son equivalentes:*

(i) *G es nilpotente de clase $c \geq 1$*

(ii) $\gamma_{c+1}G = 1$ *y* $\gamma_c G \neq 1$

(iii) $\zeta_c G = G$ *y* $\zeta_{c-1}G \neq G$.

4.4. p-Grupos finitos

un resultado clásico en teoría de grupos finitos es que todo p-grupo finito es un grupo nilpotente.

Teorema 4.4.1. *Sea p un primo arbitrario. Entonces cada p-grupo finito es nilpotente.*

Demostración. Sea p un primo. Consideremos un p-grupo finito G de orden p^n, para algún $n \in \mathbb{N}$. Tenemos que $Z(G) \neq 1$ (Teorema 3.1.2). Así, $G/Z(G)$ es un p-grupo finito de orden p^r, para algún $r \in \mathbb{N}$ tal que $r < n$. Usando otra vez el Teorema 3.1.2 $Z(G/Z(G))$ es no trivial. Por tanto $Z(G/Z(G)) = \zeta_2 G/Z(G)$ es un p-grupo de orden p^s, para algún $s \in \mathbb{N}$ tal que $s < r$. Por tanto $|Z(G)| < |\zeta_2 G|$ y $Z(G)$ es un subgrupo propio de $\zeta_2 G$. Repitiendo este porceso, tenemos que $|\zeta_i G| < |\zeta_{i+1} G|$ para $i \geq 0$, así que $\zeta_i G$ es un subgrupo propio de $\zeta_{i+1}G$ para $i \geq 0$. Como G es finito, el proceso debe terminar. Finalmente $\zeta_k G = G$, para algún $k \in \mathbb{N}$. Por lo tanto G es nilpotente. □

Ejemplo 4.4.2. El grupo diedral D_{2^n} ($n \in \mathbb{N}$, $n \geq 1$) es un 2-grupo, por tanto es nilpotente.

Ejemplo 4.4.3. El *grupo de los cuaterniones* $\mathcal{Q}$ es el grupo con presentación

$$\mathcal{Q} = \langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$

Los elementos de $\mathcal{Q}$ son $1, x, x^2, x^3, y, xy, x^2y$ y x^3y. Como $\mathcal{Q}$ tiene orden $8 = 2^3$, entonces es nilpotente.

Ejemplo 4.4.4. Si G y H son dos grupos finitos de orden m y n respectivamente, entonces el producto directo $G \times H$ y el producto semidirecto $G \rtimes_\varphi H$ por φ tiene orden mn. En particular, el producto directo y el producto semidirecto de dos p-grupos finitos es un p-grupo finito.

Observación 4.4.5. En contraste al Teorema 4.4.1, no todo p-grupo infinito debe ser nilpotente. En (1) G. Baumslag construye un p-grupo infinito no nilpotente con ayuda del producto espiral[1].

[1]Sean A y T dos grupos. Para cada $s \in T$, sea A_s una copia isomorfa de A, y sea a_s la imagen de dicho isomorfismo de A en A_s. Consideremos el producto directo $B = \prod_{s \in T} A_s$, y definamos el *producto espiral estandar (o restringido)* de A por T como

$$W = A \wr T = B \rtimes_\varphi T.$$

4.5. Producto directo de grupos nilpotentes

El producto directo de grupos nilpotentes es nilpotente. Después del Lema la prueba de este resultado.

Lema 4.5.1. *Un grupo G es nilpotente de clase $c \geq 1$ si y solo si $G/Z(G)$ es nilpotente de clase $c-1$.*

Teorema 4.5.2. *Si $\{H_1, \cdots, H_n\}$ es una familia de grupos nilpotentes de clases $c_1, \cdots, c_n$ resp., entonces el producto directo $H_1 \times \cdots \times H_n$ es nilpotente de clase $max\{c_1, \cdots, c_n\}$.*

Demostración. Probaremos el teorema para $n = 2$. Supongampos que H_1 y H_2 son dos grupos nilpotentes no triviales de clases c_1 y c_2 respectivamente y supongamos que $c_1 \geq c_2 > 0$. Probaremos esto por inducción sobre c_1. Si $c_1 = 1$, entonces H_1 y H_2 son abelianos, y así $H_1 \times H_2$ es abeliano.

Supongamos que $c_1 > 0$. Por el Lema 4.1.6,

$$\frac{H_1 \times H_2}{Z(H_1 \times H_2)} \cong \frac{H_1}{Z(H_1)} \times \frac{H_2}{Z(H_2)} \tag{4.6}$$

En la parte derecha de (4.6) tenemos el producto de dos grupos nilpotentes de clases menores que c_1. Por el Lema 4.5.1 la clase de $H_1/Z(H_1)$ es $c_1 - 1$. El resultado sigue del Lema 4.5.1. □

4.6. Grupos supersolubles

Un grupo es supersoluble (o super resoluble) si tiene una serie normal invariante donde todos los factores son grupos cíclicos. La supersolubilidad es más fuerte que la noción de solubilidad.

Definición 4.6.1. Sea G un grupo. G se dice *supersoluble* si existe una serie normal

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G \tag{4.7}$$

tal que, cada cociente G_{i+1}/G_i es cíclico.

De la Definición 4.3.6 tenemos que en un grupo soluble G_{i+1}/G_i es abeliano, por tanto, un grupo supersoluble es soluble. La contrario no siempre es cierto, un ejemplo de ello es el grupo alternante de orden 4, A_4, el cual es soluble pero no supersoluble.

Ahora enunciemos algunas propiedades de los grupos supersolubles como items de una misma Proposición.

Proposición 4.6.2.

(i) *El subgrupo derivado de un grupo supersoluble es siempre nilpotente.*

---

donde $\varphi : T \to \mathrm{Aut}(B)$ es el homomorfismo que mapea cada $t \in T$ para $\varphi(t)$, donde $\varphi(t)$ es el automorfismo de B inducido por el mapeo

$$a_s \mapsto a_{st} \text{ para todos } a \in A \text{ y } s, t \in T.$$

(ii) *Los subgrupos y cocientes de un grupo supersoluble son supersolubles.*

(iii) *Cada subgrupo maximal de un grupo supersoluble tiene índice primo.*

(iv) *Un grupo finito es supersoluble si y solo si cada subgrupo maximal tiene índice primo.*

(v) *Un grupo finito es supersoluble si y solo si cada cadena de subgrupos tiene la misma longitud.*

Definición 4.6.3. Un grupo G se dice *lagrangiano*, si para cada entero positivo n que divida a $|G|$ exista un subgrupo de G de índice n.

Tenemos algunas inclusiones (estrictas) para grupos finitos:

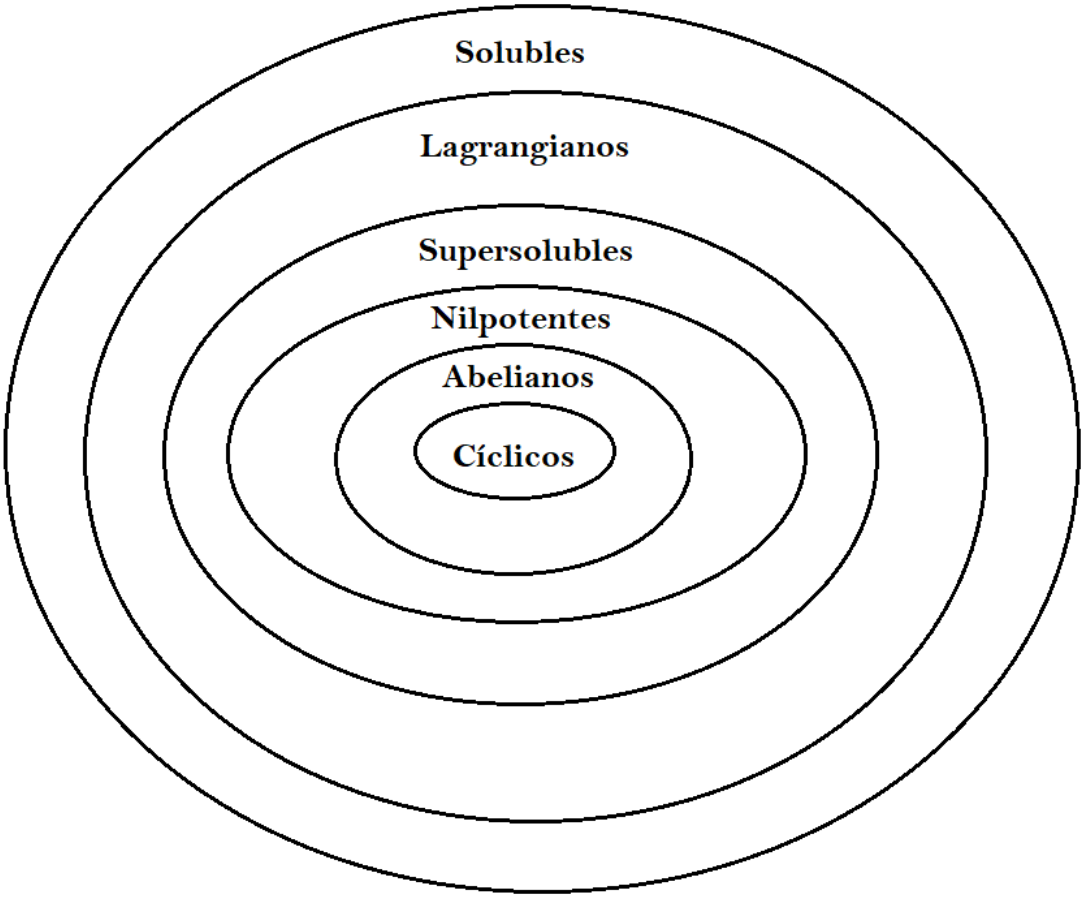


Figura 4.1: Inclusiones estrictas para grupos finitos

Capítulo 5

Grupos uniformes

Este es el capítulo con más contenido teórico que será útil en capítulos posteriores. En la sección 5.1, hablaremos sobre grupos profinitos y para el cual usaremos el concepto de límite inverso y mostraremos como un grupo de Galois es un ejemplo de un grupo profinito. En la sección 5.2, daremos tratamiento especial a los grupos pro-p y el resultado más importante es que cada grupo pro-p es el límite inverso de p-grupos finitos; daremos algunos ejemplos de estos grupos. En la sección 5.3, haremos una breve mención a los grupos procíclicos y sus equivalencias. En las secciones 5.4 y 5.5, mostraremos las principales propiedades de los p-grupos *powerful* y definiremos el rango de un grupo finito y un grupo pro-p. Los grupos uniformes serán tratados en la sección 5.6, donde definiremos su dimensión y mostraremos que $(G,+)$ es un $\mathbb{Z}_p$-módulo libre; además, vamos a estudiar los subgrupos pro-p de $\mathrm{GL}_n(\mathbb{Z}_p)$. Finalmente, en la sección 5.7 mostraremos que el $\mathbb{Z}_p$-módulo libre $(G,+)$ se torna una álgebra de Lie sobre $\mathbb{Z}_p$. El contenido de esta sección es tomada del libro 'Analytic Pro-p Groups' 2nd edn. de Dixon, J., Sautoy, M. du., Mann, A., Segal, D. (1999, pp: 15-96).

5.1. Grupos profinitos

Definición 5.1.1. Un *grupo profinito* es un grupo topológico, compacto y Hausdorff tal que sus subgrupos abiertos forman una base de vecindades para la unidad.

Proposición 5.1.2. *Sea G un grupo profinito.*

(i) *Cada subgrupo abierto de G es cerrado, tiene índice finito en G y contiene un subgrupo normal abierto de G. Un subgrupo cerrado de G es abierto si y solo si tiene índice finito. La familia de todos los subgrupos abiertos de G tiene como intersección el conjunto $\{1\}$,*

(ii) *Un subconjunto de G es abierto si y solo si es la unión de clases laterales de subgrupos normales abiertos,*

(iii) *Para cualquier subconjunto X de G*

$$\overline{X} = \bigcap_{N \lhd_o G} XN$$

Si X es un subgrupo de G, entonces

$$\overline{X} = \bigcap\{K \mid X \leq K \leq_o G\},$$

(iv) *Si X y Y son subconjuntos cerrados de G entonces el conjunto $XY = \{xy \mid x \in X, y \in Y\}$ también es cerrado. Si X es cerrado y n es un entero entonces el conjunto $\{x^n \mid x \in X\}$ es cerrado,*

(v) *Sea H un subgrupo cerrado de G. Entonces H (con la topología inducida) es un grupo profinito. Cada subgrupo abierto de H es de la forma $H \cap K$ con $K \leq_o G$,*

(vi) *Sea N un subgrupo normal cerrado de G. Entonces G/N (con la topología cociente) es un grupo profinito, y el homomorfismo natural $G \to G/N$ es una aplicación continua abierta y cerrada,*

(vii) *Una sucesión (g_i) en G converge si y solo si es una sucesión de Cauchy: i.e. para cada $N \lhd_o G$ existe $n = n(N)$ tal que $g_i^{-1}g_j \in N$ para todo $i \geq n$ y $j \geq n$.*

La demostración de esta Proposición sigue de las definiciones.

Podemos definir un grupo profinito también como un límite inverso (sección 1.3 del capítulo 1). Sea G un grupo y sea A una familia de subgrupos normales de G. Supongamos que la familia A está ordenada por inclusión. Entonces obtenemos un sistema inverso $\{(G/N)_{N\in A}\}$ cuyas aplicaciones son los epimorfismos naturales $G/N \to G/M$ siempre que $N \leq M$. Así podemos tener la siguiente proposición.

Proposición 5.1.3. *Si G es un grupo profinito entonces G es isomorfo topológicamente al $\varprojlim(G/N)_{N\lhd_o G}$. De otro lado, el límite inverso de un sistema inverso de grupos finitos es un grupo profinito.*

Demostración. Sea $L = \varprojlim(G/N)_{N\lhd_o G}$. Consideremos el homomorfismo natural $\rho : G \to \prod G/N$, dado por $\rho(g) = (gN)_{N\lhd_0 G}$. Como $\bigcap_{N\lhd_0 G} N = 1$ tenemos que ρ es inyectiva y así $\rho(G) \leq L$. Ahora, sea $(g_N N) \in L$, entonces cada colección finita de clases $g_N N$ tiene intersección no vacía y como esas clases son también subconjuntos cerrados del espacio compacto G, sigue que $\bigcap_{N\lhd_o G} g_N N$ es no vacía. Elijamos g en esa intersección. Entonces $\rho(g) = (g_N N)$, luego ρ es sobreyectiva.

Sea $P \lhd_o G$ y definamos

$$M(P) = \prod_{N\not\geq P} G/N \times \prod_{N\geq P} \{1\} \leq \prod_{N\lhd_o G} G/N,$$

así los subgrupos $M(P) \cap L$ forman una base para las vecindades de 1 en L y para cada P tenemos que $\rho^{-1}(M(P)) = P$ es abierto en G, por tanto ρ es continuo. Pero cada isomorfismo continuo entre grupos compactos Hausdorff es un isomorfismo topológico por tanto ρ es un isomorfismo topológico.

Para la otra implicación, consideremos un sistema inverso de grupos finitos $\{G_\lambda\}_{(\lambda\in I)}$ (los grupos finitos unidos con la topología discreta). Así $\prod_{\lambda\in I} G_\lambda$ es Hausdorff y por el Teorema de Tychonoff (Teorema 1.1.4 (iii) Cap. 1) es compacto. De la definición de

producto topológico, cada vecindad de 1 contiene un subgrupo de la forma $M(S) = \prod_{\lambda \notin S} G_\lambda \times \prod_{\lambda \in S}\{1\}$ para algún subconjunto finito S de I. Por tanto $\prod G_\lambda$ es un grupo profinito. Ahora solamente tenemos que mostrar que $\varprojlim G_\lambda = L$ es un subgrupo cerrado. Sea $l = (g_\lambda) \in \prod G_\lambda \backslash L$, entonces existen $\upsilon > \mu$ en I tales que $\pi_{\upsilon\mu}(g_\upsilon) \neq g_\mu$. Tenemos que $lM(\upsilon, \mu)$ es una vecindad abierta de $l \in \prod G_\lambda$ y $lM(\upsilon, \mu) \cap L = \emptyset$. Mostrando finalmente que $\prod G_\lambda \backslash L$ es abierto en $\prod G_\lambda$ y obtenemos el resultado. □

Dado un grupo topológico G, decimos que un subconjunto X de G *genera G topológicamente* si $G = \overline{\langle X \rangle}$.

Proposición 5.1.4. *Sean G un grupo profinito, H un subgrupo cerrado de G, $X \subseteq H$ y d un entero positivo. Entonces*

(i) $H = \overline{\langle X \rangle}$ si y solo si $HN/N = \overline{\langle XN/N \rangle}$ para cada $N \lhd_o G$.

(ii) Si HN/N puede ser generado por d elementos para cada $N \lhd_o G$, entonces H puede ser generado topológicamente por un subconjunto de d elementos.

Demostración. (i) Sigue de la Proposición 5.1.2 (iii). (ii) Para cada $N \lhd_o G$, sea Z_N el conjunto de todas las d-uplas de elementos de G/N que generan HN/N. Cada Z_N es finito y no vacío. Si $\pi_{MN} : G/M \to G/N$ es la proyección natural para $M \leq N$, ambos subgrupos normales abiertos de G, entonces $\pi_{MN}(Z_M) \subseteq Z_N$, y por eso $\{Z_N\}_{N \lhd_o G}$ se torna un sistema inverso. Por la Proposición 1.3.5 del capítulo 1 el límite inverso de ese sistema inverso es no vacío. Sea ahora $(X_N) \in \varprojlim Z_N$. Entonces existen $x_1, ..., x_d$ elementos en G tales que para cada $N \lhd_o G$, $X_N = (x_1 N, ..., x_d N)$ y usando la parte (i) tenemos que $\{x_1, ..., x_d\}$ genera H topológicamente. □

Un subgrupo de G es *topológicamente característico* si es invariante bajo los automorfismos de G.

Proposición 5.1.5. *Sean G un grupo profinito finitamente generado y m un entero positivo. Entonces G tiene solamente un número finito de subgrupos abiertos de índice m y cada subgrupo abierto contiene un subgrupo abierto topológicamente característico.*

Demostración. (Dixon et al, 1999: 20).

Proposición 5.1.6. *Si G es un grupo profinito finitamente generado entonces cada subgrupo abierto de G es finitamente generado.*

Demostración. Sea X un conjunto de generadores topológicos para G, y asumimos sin pérdida de generalidad que $X^{-1} = X$. Sea $H \leq_o G$ y T un transversal (conjunto de representantes de todas las clases laterales) para las clases laterales derecha de H en G tal que $1 \in T$; note que T es finito. Para cada $x \in X$ y $t \in T$ existe $s = s(t, x) \in T$ tal que $Htx = Hs$. Definamos

$$Z = \{tx \cdot s(t, x)^{-1} \mid t \in T, x \in X\},$$

y mostramos que $H = \overline{\langle Z \rangle}$.

Consideremos el subgrupo $M = \overline{\langle Z \rangle}$ de G. Si $a \in M$, $t \in T$ y $x \in X$, entonces

$$at \cdot x = atxs(t,x)^{-1} \cdot s(t,x) \in MT;$$

así $MTX = MT$. Como $1 \in MT$ y $X = X^{-1}$, sigue que $MT \supseteq \langle X \rangle$; y como T es finito MT es cerrado y por tanto $MT = G$. También $M \leq H$ y así

$$H = MT \cap H = M(T \cap H) = M.$$

Como Z es un conjunto finito, tenemos que H es finitamente generado. □

Definición 5.1.7. Sea G un grupo profinito. El *subgrupo de Frattini* de G es definido por

$$\Phi(G) = \bigcap\{M \mid M \text{ es un subgrupo abierto propio maximal de } G\}.$$

Proposición 5.1.8. *Sea G un grupo profinito.*

(i) $\Phi(G) \lhd_c G$

(ii) *Si* $K \lhd_c G$ *y* $K \leq \Phi(G)$ *entonces* $\Phi(G/K) = \Phi(G)/K$

(iii) *Para un subconjunto X de G los siguientes son equivalentes:*

  (a) X *genera G topológicamente*

  (b) $X \cup \Phi(G)$ *genera G topológicamente*

  (c) $X\Phi(G)/\Phi(G)$ *genera $G/\Phi(G)$ topológicamente.*

Demostración. (Dixon et al, 1999: 21).

Cada grupo discreto es profinito si y solo si es finito. El grupo de enteros p-ádicos y el grupo de Prüfer son también ejemplos de grupos profinitos. Ejemplos más sofisticados de grupos profinitos vienen de la Teoría de Galois.

5.1.1. Grupos profinitos como grupos de Galois

Consideramos una extensión de Galois $L|K$ (i.e. L es un cuerpo de descomposición separable posiblemente infinito de una familia de polinomios sobre un cuerpo K) entonces L es la unión $L = \bigcup\{L_i \mid i \in I\}$ de sus subextensiones finitas de Galois $L_i|K$. El conjunto $\{L_i \mid i \in I\}$ es un conjunto parcialmente ordenado por inclusión. Escribamos $i \succeq j$ cuando $L_i \supseteq L_j$. Así para el conjunto $\{L_i \mid i \in I\}$ si $i, j \in I$ existe $k \in I$ tal que $k \succeq i$ y $k \succeq j$.

Podemos definir el grupo de Galois $\mathrm{Gal}(L|K)$ como el grupo de automorfismos de L que fijan los elementos de K. Cada automorfismo $\alpha \in \mathrm{Gal}(L|K)$ está únicamente determinado por sus restricciones $\alpha|_{L_i}$ para cada $i \in I$, y la sobreyectividad de $\phi_i : \mathrm{Gal}(L|K) \to \mathrm{Gal}(L_i/K)$ es gracias a que $L|K$ y sus subextensiones $L_i|K$ son normales. En el caso de tener $i \succeq j$ entonces $(\alpha|_{L_i})|_{L_j} = \alpha|L_j$ que es llamada la *condición de compatibilidad*. Si tenemos $L_i \supseteq L_j$, en ese caso escribamos $\phi_{j,i} : \mathrm{Gal}(L_i|K) \to \mathrm{Gal}(L_j|K)$ que denota la aplicación de restricción natural, así podemos escribir la condición de compatibilidad como $\phi_i\phi_{ij} = \phi_j$ cuando $i \succeq j$. Expresemos una condición semejante en terminos de restricciones, si $i \succeq j \succeq k$ entonces $\phi_{ij}\phi_{jk} = \phi_{ik}$.

Sea el grupo de Galois $G := \mathrm{Gal}(L|K)$. Definamos $G_i := \mathrm{Gal}(L_i|K)$ y la aplicación

$$\phi : G \to \prod_{i\in I} G_i, \qquad g \mapsto (\phi_i(g))_{i\in I}$$

esta induce un isomorfismo de G sobre el grupo

$$G_\phi = \{(g_i)_{i\in I} \in \prod_{i\in I} G_i \mid \phi_{ij}(g_i) = g_j \text{ cuando } i \succeq j\}.$$

Ahora, podemos hacer una pregunta más, ¿que pasa con la correspondencia de Galois? La respuesta es que apenas ciertos subgrupos de G corresponden a los cuerpos intermediarios de $L|K$. Para responder esa pregunta y saber cuales subgrupos desempeñan un papel en la correspondencia de Galois, vamos a unir G con la *topología de Krull*. Consideremos G_i con la topología discreta, así $\prod_{i\in I} G_i$ se torna un grupo topológico totalmente disconexo, compacto y Hausdorff. Luego G_ϕ es cerrado y así G se torna un grupo topológico totalmente disconexo, compacto y Hausdorff y por tanto la estructura de G es determinada por sus imágenes finitas G_i. Además, G_ϕ es el límite inverso del sistema inverso $(G_i; \phi_{ij})$ de grupos finitos (Proposición 1.3.3 (1.1)) y por tanto G es isomorfo a un grupo profinito.

Si M es un cuerpo intermediario de la extensión $L|K$, entonces el conjunto G^M de todos los elementos de G que fijan M puede ser descrito en términos de las restricciones de los automorfismos para subextensiones finitas de M. De hecho, G^M puede ser escrito como una intersección de subgrupos abiertos-cerrados de G y por tanto es un subgrupo cerrado para la topología de Krull. Por tanto es así que la correspondencia de Galois está generalizada.

5.2. Grupos pro-p

Definición 5.2.1. Un grupo pro-p es un grupo profinito donde cada subgrupo normal abierto tiene índice igual a una potencia de p.

Proposición 5.2.2. *Sea G un grupo profinito.*

(i) *Si G es pro-p y $H \leq_c G$ entonces H es pro-p*

(ii) *Sea $K \lhd_c G$. Entonces G es pro-p si y solo si K y G/K son grupos pro-p.*

Demostración. Sigue de la definición y de la Proposición 4.1.2. □

Proposición 5.2.3. *Un grupo topológico G es un grupo pro-p si y solo si G es topológicamente isomorfo a un límite inverso de p-grupos finitos.*

Demostración. Supongamos que G es pro-p, entonces es profinito por definición y usando la Proposición 5.1.3 tenemos que

$$G \cong \varprojlim (G/N)_{N\lhd_o G}$$

siendo cada G/N un p-grupo finito. Para la otra implicación, supongamos que $G = \varprojlim (G_\lambda)_{\lambda\in I}$ donde cada G_λ es un p-grupo finito. Entonces por la Proposición 5.1.3 G es un grupo profinito y tenemos que cada subgrupo abierto de G contiene un subgrupo de la forma

$$U(M) = G \cap (\prod_{\lambda\notin M} G_\lambda \times \prod_{\lambda\in M} \{1\})$$

para algún subconjunto finito M de I. Tenemos que $|G : U(M)|| \prod_{\lambda \in M} |G_\lambda|$ y así cada subgrupo de G tiene índice igual a una potencia de p. □

Proposición 5.2.4. *Sea G es un grupo pro-p, $[G, G]$ el grupo derivado y $G^p = \langle g^p \mid g \in G \rangle$, entonces el subgrupo de Frattini de G es igual a*

$$\Phi(G) = \overline{G^p[G, G]}.$$

Demostración. (Dixon et al, 1999: 23).

Proposición 5.2.5. *Sea G un grupo pro-p. Entonces G es finitamente generado si y solo si $\Phi(G)$ es abierto en G.*

Demontración. Supongamos que $\Phi(G)$ es abierto en G. Entonces por la Proposición 5.1.2.(i) el índice de $\Phi(G)$ en G es finito y así $G/\Phi(G)$ es finito. Luego existe un subconjunto finito X de G tal que $G = X\Phi(G)$ y usando la Proposición 5.1.8.(iii) sigue que $G = \overline{\langle X \rangle}$.

Para la otra implicación, supongamos que $G = \overline{\langle X \rangle}$ donde $|X| = d$ es finito. Si $\Phi(G) \leq N \lhd_o G$ entonces G/N es un p-grupo abeliano elemental y por tanto puede ser generado por d elementos (Proposición 5.2.4); así $|G : N| \leq p^d$. Entre todos estos N vamos a escoger un subgrupo N_0 cuyo índice en G sea el mayor posible. De esto, si $\Phi(G) \leq N \lhd_o G$ tenemos que $N_0 \leq N$. Como $\Phi(G)$ es un subgrupo cerrado y normal en G sigue que

$$\Phi = \bigcap \{N \mid \Phi(G) \leq N \lhd_o G\} = N_o.$$

Así $\Phi(G)$ es abierto en G. □

Definición 5.2.6. Sea G un grupo pro-p. Definimos la *serie p-central inferior de G* en la forma siguiente:

$$P_1(G) = G$$

y para $i \geq 1$

$$P_{i+1}(G) = \overline{P_i(G)^p[P_i(G), G]}.$$

Así $P_2(G) = \Phi(G)$ (Proposición 5.2.4). Observe que $P_{i+1}(G) \geq \Phi(P_i(G))$ para cada i.

La siguiente proposición muestra que la topología de los grupos pro-p finitamente generados es determinada por su estructura de grupo. Vea la demostración de esa proposición (Dixon et al, 1999: 24).

Proposición 5.2.7. *Sea G un grupo pro-p.*

(i) *$P_i(G/K) = P_i(G)K/K$ para todo $K \lhd_c G$ y para todo i*

(ii) *$[P_i(G), P_j(G)] \leq P_{i+j}(G)$ para todo i y j*

(iii) *Si G es finitamente generado entonces $P_i(G)$ es abierto en G para todo i, y el conjunto $\{P_i(G) \mid i \geq 1\}$ es una base para las vecindades de 1 en G.*

Lema 5.2.8. *Si G es un grupo pro-p y K es un subgrupo de índice finito en G entonces $|G : K|$ es una potencia de p.*

Proposición 5.2.9. *Si G es un grupo pro-p finitamente generado entonces el grupo derivado $[G, G]$ es cerrado en G.*

De estos dos resultados sigue el teorema siguiente.

Teorema 5.2.10. *Si G es un grupo pro-p finitamente generado entonces cada subgrupo de índice finito en G es abierto.*

Demostración. Sea G un grupo pro-p finitamente generado. Escribimos $G^{\{p\}} = \{g^p \mid g \in G\}$, $G^{\{p\}}$ por ser la imagen de una función continua $(g \mapsto g^p)$ es compacto y por tanto cerrado. Como $G/[G, G]$ es abeliano entonces $G^p[G, G] = G^{\{p\}}[G, G]$ y usando la Proposición 5.2.9 $G^p[G, G]$ es cerrado y es igual a $\Phi(G)$. Por la Proposição 5.2.5 sigue que $G^p[G, G]$ es abierto en G.

Sea ahora K un subgrupo normal propio de índice finito de G. Entonces usando inducción y sin pérdida de generalidad podemos asumir que K es abierto en M siempre que M es un grupo pro-p finitamente generado con $K \leq M < G$. Tomando $M = G^p[G, G]K$, tenemos que G/K es un p-grupo finito (Lema 5.2.8); sigue que $M < G$. Como $|G : M| \leq |G : \Phi(G)| < \infty$, tenemos que M es un subgrupo abierto en G. Por tanto M es un grupo pro-p finitamente generado (Proposición 5.1.6) y usando la hipótesis inductiva; K es abierto en M. Así K es abierto en G y como cada subgrupo de índice finito en G contiene un subgrupo de la forma de K; tenemos que cada subgrupo de índice finito tiene que ser abierto. □

Una observación importante es que en el caso de un grupo pro-p *finitamente generado* podemos suprimir la "barra"de la Definición 5.2.6.

Corolario 5.2.11. *Si G es un grupo pro-p finitamente generado, entonces $\Phi(G) = G^p[G, G]$ y $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$ para cada i.*

Recientemente Nikolov y Segal mostraron que en un grupo profinito finitamente generado cada subgrupo de índice finito es abierto (Nikolov et al, 2007: 171-238); luego, la topología de un grupo profinito finitamente generado es determinado por su estructura de grupo.

Corolario 5.2.12. *Cada homomorfismo (abstracto) de un grupo pro-p finitamente generado para un grupo profinito es continuo.*

Proposición 5.2.13. *Si $H = \langle a_1, ...a_d \rangle$ es un grupo nilpotente entonces cada elemento de $[H, H]$ es igual a un producto de la forma $[x_1, a_1] \cdots [x_d, a_d]$ con $x_1, \cdots, x_d \in H$.*

Ahora vamos a mencionar algunos ejemplos de grupos pro-p.

(1) Todo p-grupo finito es un grupo pro-p

(2) Sea G el grupo de Galois de una extensión de Galois (posiblemente infinita) de un cuerpo, si todo subgrupo normal de G de índice finito tiene índice una potencia de

p, entonces G es un grupo pro-p

(3) El grupo aditivo de los enteros p-ádicos también es un grupo pro-p.

5.3. Grupos procíclicos

Vamos a ver la importancia de definir la potencia p-ádica en un grupo pro-p y notaremos que papel desempeñan los enteros p-ádicos en este sentido.

Lema 5.3.1. *Sea G un grupo pro-p y $g \in G$. Consideremos las sucesiones (a_i) y (b_i) de enteros convergentes en la topología p-ádica y tendiendo para el mismo límite en $\mathbb{Z}_p$. Entonces las sucesiones (g^{a_i}) y (g^{b_i}) convergen en G para el mismo límite.*

Demostración. Sea N un subgrupo normal y abierto en G, entonces $|G/N| = p^j$ para algún j. Si consideramos enteros i y k suficientemente grandes tenemos que $a_i \equiv a_k \ (\mathrm{mod} p^j)$ y así $g^{a_i} \equiv g^{a_k} (\mathrm{mod} N)$. Tenemos que (g^{a_i}) es una sucesión de Cauchy en G y por la Proposición 5.1.2 es convergente para un elemento en G, digamos g_1. Análogamente (g^{b_i}) converge para un elemento g_2 en G. Si k es un entero suficientemente grande entonces $b_k \equiv a_k \ (\mathrm{mod} p^j)$, $g^{b_k} \equiv g_2 \ (\mathrm{mod} N)$, así obtenemos

$$g_1 g_2^{-1} \equiv g^{a_k - b_k} \equiv 1 \ (\mathrm{mod} N),$$

y por ser N arbitrario tenemos que $g_1 = g_2$. □

Con el Lema 5.3.1 tenemos la unicidad del Límite y por tanto podemos hacer la siguiente definición.

Definición 5.3.2. Sea G un grupo pro-p, $g \in G$ y $\lambda \in \mathbb{Z}_p$. Entonces

$$g^{\lambda} = \lim_{n \to \infty} g^{a_n}$$

donde (a_n) es una sucesión de enteros con $\lim_{n \to \infty} a_n = \lambda$.

La definición de "exponenciación p-ádica" que terminamos de definir tiene las siguientes propiedades que pueden ser demostradas a partir de su propia definición.

Proposición 5.3.3. *Sea G un grupo pro-p, sean $g, h \in G$, y sean $\lambda, \mu \in \mathbb{Z}_p$. Entonces tenemos que*

(i) $g^{\lambda+\mu} = g^{\lambda} g^{\mu}$ *y* $g^{\lambda\mu} = (g^{\lambda})^{\mu}$

(ii) *Si $gh = hg$ entonces $(gh)^{\lambda} = g^{\lambda} h^{\lambda}$*

(iii) *La aplicación $\upsilon \to g^{\upsilon}$ define un homomorfismo continuo de $\mathbb{Z}_p$ para G. Su imagen $g^{\mathbb{Z}_p}$ es la cerradura en G de $\langle g \rangle$.*

Demostración. (Dixon et al, 1999: 30).

Definición 5.3.4. Un grupo G es *procíclico* si es profinito y G/N es un grupo cíclico

para cada subgrupo normal abierto N de G.

Proposición 5.3.5. *Sea G un grupo pro-p. Entonces las siguientes afirmaciones son equivalentes.*

(a) *G es procíclico*

(b) *G puede ser generado topológicamente por un subconjunto de 1-elemento*

(c) *$G = g^{\mathbb{Z}_p}$ para algún $g \in G$*

(d) *G es finito y cíclico o es topológicamente isomorfo a $\mathbb{Z}_p$.*

Demostración. $((a) \Rightarrow (b))$. Supongamos que G es un grupo procíclico y supongamos que tiene dos subgrupos propios maximales diferentes M y N. Entonces $M \cap N \geq \Phi(G) \geq G^p[G,G]$, así M y N son subgrupos normales de índice p en G y $G/(M \cap N)$ es un grupo abeliano elemental de orden p^2, pero no es un grupo cíclico. Entonces $G = 1$ o G tiene un único subgrupo propio maximal abierto; de cualquier forma en ambos casos $\Phi(G)$ es abierto en G y $G/\Phi(G)$ es cíclico. Por tanto G puede ser generado topológicamente por un conjunto de un elemento (Proposición 5.1.8). $((b) \Rightarrow (c))$ Proposición 5.3.3 (iii). $((c) \Rightarrow (d))$ Supongamos que $G = g^{\mathbb{Z}_p}$ para algún $g \in G$ y sea K el núcleo del homomorfismo $\theta : \mathbb{Z}_p \to G$ dado por $\theta(\lambda) = g^{\lambda}$, así θ es sobreyectivo por definición y por el Corolario 5.2.12 es continua. Como $\mathbb{Z}_p/K$ y G son grupos compactos Hausdorff y así G es topológicamente isomorfo a $\mathbb{Z}_p/K$. $((d) \Rightarrow (a))$ Simplemente tenemos que observar que cada grupo cociente propio de $\mathbb{Z}_p$ es cíclico. □

Todos los grupos cíclicos finitos son grupos pro-cíclicos. De la definición 5.3.4 obtenemos que el grupo de Prüfer y los enteros p-ádicos son ejemplos de grupos pro-cíclicos.

5.4. p-Grupos powerful

En esta sección vamos a prestar más atención a los p-grupos finitos. Para entender la estructura de los grupos pro-p analíticos debemos ver en las propiedades de una clase especial de grupos finitos.

Definición 5.4.1.

(i) Un p-grupo finito G es *powerful* si p es impar y G/G^p es abeliano, o si $p = 2$ y G/G^4 es abeliano,

(ii) Un subgrupo N de un p-grupo finito G es *powerfully embedded* en G, escribimos N p.e. G, si p es impar y $[N,G] \leq N^p$, o si $p = 2$ y $[N,G] \leq N^4$.

Por tanto G es powerful si y solo si G p.e. G; y si N p.e. G entonces $N \lhd G$ y N es powerful. Cuando p es impar G es powerful si y solo si $G^p = \Phi(G)$.

Lema 5.4.2. *Sea G un p-grupo finito y sean N, K y W subgrupos normales de G tales que $N \leq W$.*

(i) *Si N p.e. G entonces NK/K p.e. G/K,*

(ii) *Si p es impar y $K \leq N^p$, o si $p = 2$ y $K \leq N^4$, entonces N p.e. G si y solo si N/K p.e. G/K,*

(iii) *N p.e. G y $x \in G$ entonces $\langle N, x\rangle$ es powerful,*

(iv) *Si N no es powerfully embedded en W, entonces existe un subgrupo normal J de G tal que*

- *si p es impar,*

$$N^p[N,W,W] \leq J \leq N^p[N,W] \qquad \text{y} \qquad |N^p[N,W] : J| = p;$$

- *si $p = 2$,*

$$N^4[N,W]^2[N,W,W] \leq J \leq N^4[N,W] \qquad \text{y} \qquad |N^4[N,W] : J| = 2.$$

Demostración. (i), (ii) Usar solo la definición. (iii) Definimos $H = \langle N, x\rangle$. Como $N \lhd H$ tenemos $[H,H] = [N,H]$, por hipótesis tenemos que N p.e. G y por tanto $[H,H] \leq N^p \leq H^p$ (respectivamente $[H,H] \leq H^4$ si $p = 2$). (iv) Supongamos que p es impar y que $[N,W] \not\leq N^p$, entonces $N^p \lneq N^p[N,W] = M$. Sabemos que G es un p-grupo y tanto M como N son normales en G entonces existe un $J \lhd G$ tal que $N^p \leq J \lneq M$ y $|M : J| = p$. Por tanto M/J es central en G/J y tenemos el resultado (proceder de la misma forma para el caso $p = 2$). □

Proposición 5.4.3. *Sea G un p-grupo finito y $N \leq G$. Si N p.e. G entonces N^p p.e. G.*

Demostración. (Dixon et al, 1999: 38).

Observe que si G fuese un p-grupo finito, entonces:

$$P_1(G) = G, \quad P_{i+1}(G) = P_i(G)^p[P_i(G), G] \ \text{ para cada } \ i \geq 1.$$

Para el resto de la sección vamos a escribir simplemente $G_i = P_i(G)$.

Lema 5.4.4. *Sea G un p-grupo finito powerful.*

(i) *Para cada i, G_i p.e. G y $G_{i+1} = G_i^p = \Phi(G_i)$*

(ii) *Para cada i, la aplicación $x \to x^p$ induce un epimorfismo de G_i/G_{i+1} para G_{i+1}/G_{i+2}.*

Demostración. (i) Tenemos que $G = G_1$ es powerful, así G_1 p.e. G. Supongamos que G_i p.e G para algún $i \geq 1$. Entonces $G_{i+1} = G_i^p[G_i, G] = G_i^p$, y G_{i+1} p.e. G (Proposición 5.4.3) pero $G_i^p \leq \Phi(G_i) = G_i^p[G_i, G_i] \leq G_{i+1}$ y así $G_{i+1} = \Phi(G_i)$. Entonces aplicando inducción tenemos el resultado.
(ii) Por la parte (i) podemos mostrar que G_i es powerful, $G_{i+1} = P_2(G_i)$ y $G_{i+2} = P_3(G_i)$. Vamos a suponer que $i = 1$ y hacemos el cambio de G por G/G_3; aquí podemos suponer que $G_3 = 1$. Por tanto $[G,G] \leq G_2 \leq Z(G)$, así para $x, y \in G$ tenemos que

$$(xy)^p = x^p y^p [x,y]^{p(p-1)/2},$$

si p es impar tenemos que $p|(p(p-1)/2)$, así

$$[y,x]^{p(p-1)/2} \in G_2^p = G_3 = 1,$$

Si $p = 2$ entonces $[G, G] \leq G^4 \leq G_3 = 1$. Así en cualquier caso tenemos que $(xy)^p = x^p y^p$. Como $G_2^p = G_3 = 1$ y $G^p = G_2$, esto muestra que $x \mapsto x^p$ induce un homomorfismo de G/G_2 para G_2/G_3. □

Lema 5.4.5. *Si $G = \langle a_1, ..., a_d \rangle$ es un p-grupo finito powerful, entonces $G^p = \langle a_1^p, ..., a_d^p \rangle$.*

Demostración. (Dixon et al, 1999: 40).

Proposición 5.4.6. *Si G es un p-grupo finito powerful entonces cada elemento de G^p es una p-ésima potencia en G.*

Demostración. La prueba es por inducción sobre $|G|$. Sea $g \in G^p$. Entonces existen $x \in G$ y $y \in G_3$ tales que $g = x^p y$ (Lema 5.4.4). Definamos $H = \langle G^p, x \rangle$. Por el Lema 5.4.4, $G^p = G_2$ p.e. G y por el Lema 5.4.2 (iii) H es powerful. Además, como $y \in G_3 = G_2^p$; tenemos que $g \in H^p$. Supongamos que $H \neq G$. Entonces por la hipótesis inductiva g es una p-ésima potencia en H. Supongamos ahora que $H = G$. Como $G = \langle G^p, x \rangle = \Phi(G)\langle x \rangle$, tenemos que G es cíclico. En ese caso es claro que G es una p-ésima potencia en G. Eso termina la prueba. □

Podemos ahora resumir la principal característica de una serie p-inferior en un p-grupo powerful.

Teorema 5.4.7. *Sea $G = \langle a_1, \cdots, a_d \rangle$ un p-grupo finito powerful y sea $G_i = P_i(G)$ para cada i. Entonces:*

(i) *G_i p.e. G*

(ii) *$G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$, para cada $k \geq 0$*

(iii) *$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle$*

(iv) *la aplicación $x \to x^{p^k}$ induce un homomorfismo de G_i/G_{i+1} para G_{i+k}/G_{i+k+1}, esto es para cada i y k.*

Demostración. (Dixon et al, 1999: 40).

Corolario 5.4.8. *Si $G = \langle a_1, \cdots, a_d \rangle$ es un p-grupo finito powerful entonces $G = \langle a_1 \rangle \cdots \langle a_d \rangle$, i.e. G es el producto de sus subgrupos cíclicos $\langle a_i \rangle$.*

Demostración. (Dixon et al, 1999: 41).

Para un p-grupo finito G, definimos por $d(G)$ la menor cardinalidad de un conjunto de generadores de G. Así $d(G)$ es también la dimensión de $G/\Phi(G)$ como un espacio vectorial sobre $\mathbb{F}_p$.

Teorema 5.4.9. *Si G es un p-grupo powerful y $H \leq G$ entonces $d(H) \leq d(G)$.*

Demostración. Probaremos esto por inducción sobre $|G|$. Supongamos que el resultado es válido para los p-grupos powerful con el orden menor que el orden de G. Definamos d=d(G) y m =d(G_2). Entonces G_2 es powerful (Lema 5.4.4 (i)) y usando la hipótesis

inductiva tenemos que el subgrupo $K = H \cap G_2$ satisface $\mathrm{d}(K) \leq m$. Consideramos la aplicación $\pi : G/G_2 \to G_2/G_3$ dada por $x \mapsto x^p$, esta aplicación es un epimorfismo (Lema 5.4.4 (ii)) y $\dim(\ker\pi) = d - m$. Así $\dim(\ker\pi \cap HG_2/G_2) \leq d - m$. Luego

$$\dim(\pi(HG_2/G_2)) \geq \dim(HG_2/G_2) - (d - m) = m - (d - r);$$

donde $r = \dim(HG_2/G_2)$. Sean $h_1, \cdots, h_r$ elementos en H tales que $HG_2 = \langle h_1, ..., h_r\rangle G_2$. Sabemos que $\Phi \leq K^p \leq G_3$. Entonces el subespacio formado por las clases laterales $h_1^p, ..., h_r^p$ tienen dimensión al menos $\dim((HG_2/G_2)\pi) \geq m - (d - r)$ y como $\mathrm{d}(K) \leq m$ podemos entonces encontrar $d - r$ elementos $y_1, ..., y_{d-r} \in K$ tales que

$$K = \langle h_1^p, \cdots, h_r^p, y_1, \cdots, y_{d-r}\rangle\Phi(K).$$

Entonces $K = \langle h_1^p, \cdots, h_r^p, y_1, \cdots, y_{d-r}\rangle$ y así tenemos que

$$H = H \cap \langle h_1, \cdots, h_r\rangle G_2 = \langle h_1, \cdots, h_r\rangle K = \langle h_1, \cdots, h_r, y_1, \cdots, y_{d-r}\rangle$$

Por tanto $\mathrm{d}(H) \leq d$. □

El *rango* de un grupo finito G es definido por:

$$rk(G) = \sup\{d(H) \mid H \leq G\}. \tag{5.1}$$

Por (1,1) y usando el Teorema 5.4.9 podemos decir que si G *es un p-grupo powerful entonces* $rk(G) = d(G)$.

Definición 5.4.10. Para un p-grupo finito G y un entero positivo r, $V(G, r)$ denota la intersección de los núcleos de todos los homomorfismos de G para $GL_r(\mathbb{F}_p)$.

Definición 5.4.11. Un grupo G es metacíclico si contiene un subgrupo cíclico N, tal que G/N es también cíclico.

Proposición 5.4.12. *Si p es impar entonces cada p-grupo metacíclico finito es powerful.*

Demostración. Sea G un p-grupo metacíclico finito. Entonces contiene un subgrupo cíclico $N = \langle x\rangle$ tal que $G/N = \langle yN\rangle$ es cíclico. Si $b \in G$ el puede ser escrito como $y = x^n y^m$. Entonces $G = \langle x, y\rangle$. Como N es cíclico entonces $N \lhd G$ y G/N es abeliano por ser cíclico. Luego $[G, G] \subseteq N$. Como $\{x, y\}$ genera G entonces $[x, y]$ genera a $[G, G]$. Así $\langle[x, y]\rangle = [G, G] \subseteq N$ y por tanto $[x, y] = x^{p^e}$ para algún entero no negativo e. Luego $[G, G] \subseteq G^p$ y G es powerful. □

Observación 5.4.13. En verdad podemos considerar a los p-grupos "powerful" como generalizaciones de los p-grupos finitos abelianos.

Algunos ejemplos de grupos powerful.

(i) Todo p-grupo finito abeliano es un p-grupo powerful,

(ii) Consideremos el grupo $\mathbb{Z}/10\mathbb{Z}$. Este contiene un subgrupo isomorfo al grupo cíclico $\mathbb{Z}/2\mathbb{Z}$ y el subgrupo cociente es isomorfo a $\mathbb{Z}/5\mathbb{Z}$, que es también cíclico. Por la Proposición 5.4.12, $\mathbb{Z}/10\mathbb{Z}$ es un p-grupo metacíclico finito y así un p-grupo powerful,

(iii) El primer ejemplo de un grupo powerful no cíclico es el grupo de Klein Dih_2. Y el grupo powerful no abeliano más pequeño es Dih_3 (la prueba de estos es usando la Proposición 5.4.12).

5.5. Grupos pro-p de rango finito

Definición 5.5.1. Sea G un grupo pro-p.

(i) G es *powerful* si p es impar y $G/\overline{G^p}$ es abeliano, o si $p = 2$ y $G/\overline{G^4}$ es abeliano

(ii) Sea $N \leq_o G$. Entonces N es *powerfully embedded* en G, escribimos N p.e. G, si p es impar y $[N, G] \leq \overline{N^p}$, o si $p = 2$ y $[N, G] \leq \overline{N^4}$.

Observe que si N p.e. G entonces $N \lhd_o G$ y N es powerful. Como $\overline{N^p}$ (resp. $\overline{N^4}$) es la intersección de todos los subgrupos normales abiertos de G en los cuales N^p (resp. N^4) está contenido.

Proposición 5.5.2. *Sea G un grupo pro-p y N un subgrupo normal abierto en G. Entonces N p.e. G si y solo si NK/K p.e. G/K para cada K subgrupo normal abierto en G.*

Corolario 5.5.3. *Sea G un grupo topológico. Entonces G es un grupo pro-p powerful si y solo si G es el límite inverso de un sistema inverso de p-grupos finitos powerful donde todas las aplicaciones son sobreyectivas.*

Lema 5.5.4. *Sea G un grupo pro-p finitamente generado powerful. Entonces cada elemento de G^p es una p-ésima potencia en G, y $G^p = \Phi(G)$ es abierto en G. Si $p = 2$, entonces G^4 es abierto en G.*

Demostración. (Dixon et al, 1999: 49).

Corolario 5.5.5. *Sea G como en el Lema 5.5.4. Entonces para cada i tenemos*

$$G^{p^i} = (G^{p^{i-1}})^p = \{x^{p^i} \mid x \in G\} \quad p.e. \quad G^{p^{i-1}} \tag{5.2}$$

Teorema 5.5.6. *Sea $G = \overline{\langle a_1, ..., a_d \rangle}$ un grupo pro-p finitamente generado powerful y definamos $G_i = P_i(G)$ para cada i. Entonces:*

(i) G_i *p.e.* G

(ii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$ *para cada* $k \geq 0$

(iii) $G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \overline{\langle a_1^{p^{i-1}}, ..., a_d^{p^{i-1}} \rangle}$

(iv) *la aplicación* $x \to x^{p^k}$ *induce un homomorfismo de* G_i/G_{i+1} *para* G_{i+k}/G_{i+k+1} *para cada* i *y* k.

Proposición 5.5.7. *Si* $G = \overline{\langle a_1, \cdots, a_d \rangle}$ *es un grupo pro-p powerful entonces* $G = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$, *i.e.* G *es el producto de sus subgrupos procíclicos* $\overline{\langle a_1 \rangle}, \cdots, \overline{\langle a_d \rangle}$.

Demostración. El conjunto $A = \overline{\langle a_1 \rangle}, \cdots, \overline{\langle a_d \rangle}$ es compacto (pues es el producto de un número finito de conjuntos cerrados y por tanto compactos), y por eso es cerrado en G. Así $A = \bigcap_{N \lhd_o G} AN$. También tenemos que $AN/N = G/N$ (Corolario 5.4.8) para cada N subgrupo normal abierto en G y por tanto $A = G$. □

Para cada grupo topológico G, $d(G)$ denota la menor cardinalidad de un conjunto de generadores topológicos de G. Si G es un grupo pro-p finitamente generado, entonces tenemos

$$d(G) = \dim_{\mathbb{F}_p}(G/\Phi(G)). \tag{5.3}$$

Usando el Teorema 5.4.9 y la Proposición 5.1.4, obtenemos el siguiente teorema.

Teorema 5.5.8. *Sea* G *un grupo pro-p finitamente generado powerful y* H *un subgrupo cerrado de* G. *Entonces* $d(H) \leq d(G)$.

En la siguiente proposición mostramos las equivalentes definiciones de "rango".

Proposición 5.5.9. *Sea* G *un grupo profinito, y sean:*

$$\begin{aligned} r_1 &= sup\{d(H) \mid H \leq_c G\} \\ r_2 &= sup\{d(H) \mid H \leq_c G \text{ y } d(H) < \infty\} \\ r_3 &= sup\{d(H) \mid H \leq_o G\} \\ r_4 &= sup\{rk(G/N) \mid N \lhd_o G\} \end{aligned}$$

entonces $r_1 = r_2 = r_3 = r_4$.

Demostración. (Dixon et al, 1999: 51).

Definición 5.5.10. Sea G un grupo profinito. El *rango* $rk(G)$ de G es cualquiera de los r_i dados en la Proposición 5.5.9.

Observe que por definición un grupo profinito de rango finito es finitamente generado. Si G es un grupo pro-p finitamente generado powerful, entonces el Teorema 5.5.8 muestra que rk(G) =d(G) y así G tiene rango finito. Generalizando, si G es finitamente generado y posee un subgrupo powerful abierto entonces G tiene rango finito. El siguiente resultado es el principal de esta sección.

Teorema 5.5.11. *Sea* G *un grupo pro-p. Entonces* G *tiene rango finito si y solo si* G *es finitamente generado y* G *posee un subgrupo powerful abierto. En estas condiciones,* G *posee un subgrupo característico powerful abierto.*

Demostración. (Dixon et al, 1999: 52).

Corolario 5.5.12. *Sea G un grupo pro-p y sea r un entero positivo. Supongamos que cada subgrupo abierto de G contiene un subgrupo abierto normal N de G con $d(N) \leq r$. Entonces G tiene rango finito.*

Teorema 5.5.13. *Sea G un grupo pro-p. Entonces las siguientes propiedades son equivalentes:*

(a) *existe $s \in \mathbb{N}$ y $c > 0$ tal que $|G : \overline{G^{p^k}}| \leq cp^{ks}$ para todo k*

(b) *existe $s \in \mathbb{N}$ y $c > 0$ tal que $|G : G^{p^k}| \leq cp^{ks}$ para todo k*

(c) G tiene rango finito.

Demostración. $((c) \Rightarrow (b))$. Supongamos que G tiene rango finito r. Entonces G posee un subgrupo normal abierto powerful H. Definamos $H_i = P_i(H)$ para cada i. Entonces tenemos que $|H : H_2| \leq p^r$ y $|H : H_{k+1}| \leq p^{kr}$ para todo k (Proposición 5.5.6 (iv)). Además, $H_{k+1} = H^{p^k}$ (Teorema 5.5.6 (iii)) y así tenemos que

$$|G : G^{p^k}| \leq |G : H^{p^k}| \leq |G : H| p^{kr}.$$

$((b) \Rightarrow (a))$ Es simplemente notar que $|G : \overline{G^{p^k}}| \leq |G : G^{p^k}|$ y el resultado es obvio. $((a) \Rightarrow (c))$ Supongamos que tenemos (a). Entonces $|G : \Phi(G)| \leq |G : \overline{G^p}| \leq cp^s$ es finito y por tanto G es finitamente generado. Definimos $W = V(G, s)$ si p es impar y $W = V(G, s)^2$ si $p = 2$. Escribamos $G_i = \overline{G^{p^i}}$ para cada i. Como W es un subgrupo normal abierto de G existe un m tal que $G_m \leq W$ y por la hipótesis inductiva tenemos que $|G_k : G_{k+1}| \leq p^s$ para algún $k \geq m$. Si no fuese así, entonces existiría un n suficientemente grande tal que

$$|G : G_{m+n}| \geq |G_m : G_{m+n}| \geq p^{s+1} n > cp^{ms} p^{ns} = cp^{(m+n)s},$$

contradiciendo nuestra hipótesis. Escogiendo un k y definiendo $K = G_k$ tenemos que $\Phi(K) \geq \overline{K^p} \geq G_{k+1}$, así $|K/\Phi(K)| \leq p^s$ y $\mathrm{d}(K) \leq s$. Finalmente K es powerful y $\mathrm{rk}(K) = \mathrm{d}(K) \leq s$ (Teorema 5.5.8).

Teorema 5.5.14. *Sea G un grupo pro-p. Entonces las siguientes afirmaciones son equivalentes:*

(a) *G es el producto de un número finito de subgrupos procíclicos*

(b) *G es el producto de un número finito de subgrupos cerrados de rango finito*

(c) *G tiene rango finito*

(d) *G es finitamente generado como un "$\mathbb{Z}_p$-grupo powerful", i.e. G tiene un subconjunto finito X tal que cada elemento de G es igual a un producto de la forma $x_1^{\lambda_1}, \cdots, x_s^{\lambda_s}$ con $x_j \in X$ y $\lambda_j \in \mathbb{Z}_p$.*

Ejemplo 5.5.15. Consideremos al grupo $\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. Este grupo unido con la topología discreta es un grupo de rango finito pues es finitamente generado y contiene un subgrupo isomorfo a $\mathbb{Z}/10\mathbb{Z}$ que en la sección anterior mostramos que es un p-grupo powerful.

5.6. Grupos uniformes

Ahora daremos la definición de un grupo uniforme y sus propiedades.

Definición 5.6.1. Un grupo pro-p G se dice *uniforme* o *uniformemente powerful* si:

(i) G es finitamente generado

(ii) G es powerful, y

(iii) $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$, para cada i.

Podemos suponer que un grupo G pro-p satisface (i) y (ii) y reformular (iii). Así en su lugar podemos escribir "la aplicación $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$ inducida por la aplicación $x \mapsto x^p$ es un isomorfismo para cada i".

Teorema 5.6.2. *Sea G un grupo pro-p finitamente generado powerful. Entonces existe un k suficientemente grande tal que $P_k(G)$ es uniforme.*

Demostración. Definamos $G_i = P_i(G)$ y supongamos que $|G_i : G_{i+1}| = p^{d_i}$ entonces tenemos que $d_1 \geq d_2 \geq \cdots \geq d_i \geq d_{i+1} \geq \cdots$ (Teorema 5.5.6 (iv)). Así existe m tal que $d_k = d_m$ para todo $k \geq m$. Además, $P_i(G_k) = G_{k+i-1}$ para todo i y k (Teorema 5.5.6 (ii)) y por tanto G_k es uniforme (Teorema 5.5.6 (i)). □

Corolario 5.6.3. *Un grupo pro-p de rango finito tiene un subgrupo característico abierto uniforme.*

Con ayuda del Teorema 5.5.6 y del Teorema 4.5.8 tenemos que un grupo powerful G es uniforme si y solo si $d(G_i/G_{i+1}) = d(G_1/G_2) = d$ para todo i.

Proposición 5.6.4. *Sea G un grupo pro-p finitamente generado powerful. Entonces las siguientes afirmaciones son equivalentes.*

(a) *G es uniforme*

(b) *$d(P_i(G)) = d(G)$ para cada $i \geq 1$*

(c) *$d(H) = d(G)$ para cada subgrupo powerful abierto H en G.*

Una caracterización de un grupo uniforme es la siguiente.

Teorema 5.6.5. *Sea G un grupo pro-p finitamente generado powerful. Entonces G es uniforme si y solo si es libre de torsión.*

Demostración. Sea G un grupo pro-p finitamente generado powerful y definamos $G_i = P_i(G)$ para todo i. Vamos a suponer que G no es libre de torsión. Entonces G contiene un elemento x de orden p. Si $x \in G_i \backslash G_{i+1}$ entonces $1 \neq xG_{i+1} \in G_i/G_{i+1}$ y $1 = x^p G_{i+2} \in G_{i+1}/G_{i+2}$. Por tanto la aplicación $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ no es inyectiva y así G no es uniforme.

Para la otra implicación, supongamos que G no es uniforme. Entonces f_i no es inyectivo para algún i y así existe $x \in G_i \backslash G_{i+1}$ tal que $x^p \in G_{i+2}$. Definamos $x_2 = x$ y

supongamos que para algún $n \geq 2$ podemos encontrar $x_2, \cdots, x_n$ satisfaciendo $x_j^p \in G_{i+j}$ y $x_j \equiv x_{j-1} \,(\mathrm{mod} G_{i+j-2})$ para $2 < j \leq n$. Entonces existe $y \in G_{i+n-1}$ tal que $x_n^p = y^p$. Definamos $x_{n+1} = y^{-1}x_n$. Entonces $x_{n+1} \equiv x_n \,(\mathrm{mod} G_{i+n-1})$ y también $x_{n+1}^p \in G_{i+n+1}$. Por tanto $x_{n+1}^p \equiv 1 \,(\mathrm{mod} G_{i+n+1})$. Así podemos construir una sucesión $x_2, \cdots, x_n, \cdots$ de Cauchy convergente para algún $\overline{x} \in G$. Por tanto $\overline{x} \equiv x \not\equiv 1 \,(\mathrm{mod} G_{i+1})$ y $\overline{x}^p \equiv x_n^p \equiv 1 \,(\mathrm{mod} G_{i+n-1})$ para todo n, y así $\overline{x}^p = 1$, lo que muestra que G no es libre de torsión. □

Lema 5.6.6. *Si A y B son subgrupos abiertos uniformes de algún grupo pro-p G. Entonces $d(A) = d(B)$.*

Demostración. Sea i un número suficientemente grande tal que $P_i(B) \leq A \cap B \leq A$ y usando la Proposición 5.6.4 tenemos que $\mathrm{d}(A) = \mathrm{d}(P_i(B)) = \mathrm{d}(B)$. □

Definición 5.6.7. Sea G un grupo pro-p de rango finito y sea H un subgrupo uniforme abierto arbitrario en G. La *dimensión* de G es definida por

$$\dim(G) = d(H). \tag{5.4}$$

Teorema 5.6.8. *Sea G un grupo pro-p de rango finito y N un subgrupo normal cerrado de G. Entonces*

$$\dim(G) = \dim(N) + \dim(G/N) \tag{5.5}$$

(observe que N y G/N tienen rango finito).

Demostración. (Dixon et al, 1999: 64).

Teorema 5.6.9. *Sea G un grupo pro-p uniforme y $d = d(G)$. Supongamos que G es generado topológicamente por el conjunto finito $\{a_1, ..., a_d\}$. Entonces la aplicación*

$$\begin{aligned} \psi : \mathbb{Z}_p^d &\longrightarrow G \\ (\lambda_1, ..., \lambda_d) &\longmapsto a_1^{\lambda_1} ... a_d^{\lambda_d} \end{aligned}$$

es un homeomorfismo.

Demostración. Sea $\{a_1, \cdots, a_d\}$ un conjunto de generadores topológicos de G. Así $G = \overline{\langle a_1, \cdots, a_d \rangle}$. Entonces $G = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$ (Proposición 5.5.7). Si $a \in G$ tenemos que $a = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$ con $\lambda_1, \cdots, \lambda_d \in \mathbb{Z}_p$. Sea k fijo y arbitrario. El grupo G/G_{k+1} tiene orden p^{kd} y $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \cdots \langle a_d G_{k+1} \rangle$, donde cada subgrupo cíclico tiene orden p^k. Entonces cada elemento de G/G_{k+1} puede ser escrito como $a_1^{e_1} \cdots a_d^{e_d} G_{k+1}$ donde $e_1, \cdots, e_d$ son enteros únicamente determinados módulo p^k. Eso implica que $\lambda_1, \cdots, \lambda_d$ son únicamente determinados módulo p^k, para cada k. Así $\lambda_1, \cdots, \lambda_d$ son enteros p-ádicos únicamente determinados. Obtenemos que la aplicación $\theta : G \to \mathbb{Z}_p^d$ dada por $\theta(a) = (\lambda_1, \cdots, \lambda_d)$ es una biyección y por el Corolario 5.2.12 es continua. Tenemos que $\psi : \mathbb{Z}_p^d \to G$ es la biyección recíproca, donde $\psi(\lambda_1, \cdots, \lambda_d) = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$. Como la multiplicación en G es continua. Entonces ψ es continua. Así ψ es homeomorfismo. □

Lema 5.6.10. *Sea G un grupo pro-p uniforme y para cada $n \in \mathbb{N}$ la aplicación $x \mapsto x^{p^n}$ es un homeomorfismo de G para G_{n+1}. Además, para cada k y m en $\mathbb{N}$, la restricción de este homeomorfismo es una biyección de G_k para G_{k+n} e induce una biyección de G_k/G_{k+m}*

para G_{n+k}/G_{n+k+m}.

Demostración. (Dixon et al, 1999: 66).

Los autores nos dicen sobre la importancia de este lema; y es que cada elemento $x \in G_{n+1}$ tiene una única p^n-ésima raíz en G, que vamos a denotar por $x^{p^{-n}}$, para esto vamos a aprovechar la biyección entre G y G_{n+1}. Así podemos usar la operación de grupo de G_{n+1} en G. De esa forma definimos una nueva estructura de grupo en G (Dixon et al, 1999: 66).

Para $x, y \in G$ definimos:

$$x +_n y = (x^{p^n} y^{p^n})^{p^{-n}};$$

así, la aplicación $x \to x^{p^{-n}}$ se torna un homomorfismo de grupos entre G_{n+1} y $(G, +_n)$.

Lema 5.6.11. Si $n > 1$, $x, y \in G$, y $u, v \in G$ entonces:

$$xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \pmod{G_n},$$

y para todo $m > n$

$$x +_m y \equiv x +_n y \pmod{G_{n+1}}.$$

Demostración. (Dixon et al, 1999: 66).

Definición 5.6.12. Sea G un grupo pro-p uniforme y sean $x, y \in G$. Definimos una nueva operación (suma en G) por

$$x + y = \lim_{n\to\infty} x +_n y; \tag{5.6}$$

a partir de esa definición tenemos que $x + y \equiv x +_n y \pmod{G_{n+1}}$ y si $u, v \in G_n$ entonces $xu + yv \equiv x + y \pmod{G_n}$

Observemos que un grupo pro-p uniforme G con la operación $+$ es un grupo abeliano con elemento identidad 1 y el elemento inverso es dado por $x \mapsto x^{-1}$.

Lema 5.6.13. *Sea G un grupo pro-p uniforme y sean x, y elementos de G. Entonces:*

(i) *Si $xy = yx$ entonces $x + y = xy$*

(ii) *Para cada entero m, $mx = x^m$*

(iii) *Para cada $n \geq 1$, $p^{n-1}G = G_n$*

(iv) *Si $x, y \in G_n$ entonces $x + y \equiv xy \pmod{G_{n+1}}$.*

Demostración. (Dixon et al, 1999: 68).

Ahora vamos a listar rápidamente otros resultados importantes; para las demostraciones consultar "Cohomology of Numbers Fields" 2nd ed, de J. Neukirch et al.

(i) Sea G un grupo pro-p uniforme y $n \in \mathbb{N}$, entonces G_n es un subgrupo aditivo de G, y las clases laterales aditivas de G_n en G son las mismas que las clases laterales multiplicativas de G_n en G. También la aplicación identidad $G_n/G_{n+1} \to G_n/G_{n+1}$ es un isomorfismo del grupo aditivo G_n/G_{n+1} para el grupo multiplicativo G_n/G_{n+1}, y el índice de G_n en el grupo aditivo $(G,+)$ es igual a $|G : G_n|$.

(ii) $(G,+)$ es un grupo pro-p uniforme de dimensión $d = d(G)$ (con la topología inicial). Además, cualquier conjunto de generadores topológicos para G es un conjunto de generadores topológicos para $(G,+)$.

(iii) Sea G un grupo pro-p uniforme de dimensión d, y sea $\{a_1, ..., a_d\}$ un conjunto de generadores topológicos para G. Entonces, con las operaciones antes definidas, $(G,+)$ es un $\mathbb{Z}_p$-módulo libre con la base $\{a_1, ..., a_d\}$.

(iv) Sea G un grupo pro-p uniforme de dimensión d. Entonces la acción de $Aut(G)$ sobre G es $\mathbb{Z}_p$-lineal con respecto a la estructura de $\mathbb{Z}_p$-módulo sobre $(G,+)$. Por tanto $Aut(G)$ puede ser definido como un subgrupo de $GL_d(\mathbb{Z}_p)$.

(v) Sea G un grupo pro-p de rango finito de dimensión d. Entonces para algún $e \leq d$ y algún p-grupo finito F existe una sucesión exacta

$$1 \to \mathbb{Z}_p^e \to G \to GL_d(\mathbb{Z}_p) \times F.$$

(vi) Sea G un grupo pro-p powerful finitamente generado. Entonces los elementos de orden finito de G forman un subgrupo característico T de G. También T es un p-grupo finito powerful y G/T es uniforme.

EJEMPLOS DE GRUPOS UNIFORMES

(1) El grupo aditivo de enteros p-ádicos es un grupo uniforme. Además, todo grupo abeliano pro-p finitamente generado y libre de torsión es un grupo pro-p uniforme; en otras palabras $\mathbb{Z}_p^n$ donde n es un entero positivo es un grupo pro-p uniforme.

(2) Ahora vamos a mostrar que el grupo $\mathrm{GL}_n(\mathbb{Z}_p)$ contiene varios ejemplos no triviales de grupos pro-p uniformes.

El grupo $\mathrm{GL}_d(\mathbb{Z}_p)$

Sea d un entero positivo y sea $M_d(\mathbb{Z}_p)$ el espacio topológico de las matrices $d \times d$ sobre $\mathbb{Z}_p$. Definimos $\Gamma = \mathrm{GL}_d(\mathbb{Z}_p)$ el subespacio topológico de $M_d(\mathbb{Z}_p)$ de todas las matrices $d \times d$ invertibles. Entonces Γ es un grupo topológico Hausdorff con la topología p-ádica (Observación 2.1.2). Dado un elemento a en $M_d(\mathbb{Z}_p)$, tenemos que $a \in \Gamma$ si y solo si $\det a \not\equiv 0 \pmod{p}$. Entonces Γ es al mismo tiempo un subespacio cerrado y abierto de $M_d(\mathbb{Z}_p)$ pues cada matriz $b \equiv a \pmod{p}$ satisface $b \in \Gamma$ si y solo si $a \in \Gamma$; esto muestra que Γ es la unión de como máximo p^{d^2} clases aditivas de $pM_d(\mathbb{Z}_p)$. Por tanto Γ es compacto. Una base para las vecindades de 1 en Γ es dada por los "subgrupos de congruencia"

$$\Gamma_i = \{\gamma \in \Gamma \mid \gamma \equiv 1_d \pmod{p^i}\},$$

para $i \geq 0$. Como $\Gamma/\Gamma_i \cong \mathrm{GL}_d(\mathbb{Z}/p^i\mathbb{Z})$ para $i \geq 1$, tenemos que

$$\begin{aligned} |\Gamma : \Gamma_1| &= (p^d - 1)(p^d - p)\cdots(p^d - p^{d-1}) \quad \text{y} \\ |\Gamma_1 : \Gamma_i| &= p^{d^2(i-1)} \text{ para } i \geq 1. \end{aligned}$$

Así Γ es profinito y Γ_1 es un grupo pro-p.

Cuando vamos a definir el concepto de grupo p-ádico analítico en el capítulo 6 notaremos que Γ es un grupo p-ádico analítico compacto; una propiedad fundamental de tales grupos es que ellos contienen un subgrupo pro-p powerful abierto finitamente generado y ahora verificamos eso directamente para $\Gamma = \mathrm{GL}_d(\mathbb{Z}_p)$.

Lema. *Sea p primo; si $p > 2$ y $n \geq 2$, o si $p = 2$ y $n \geq 3$, entonces todo elemento de Γ_n es una p-ésima potencia de un elemento en Γ_{n-1}.*

Demostración. Tenemos que mostrar que para cualquier $a \in M_d(\mathbb{Z}_p)$ podemos resolver

$$1 + p^n a = (1 + p^{n-1}x)^p \tag{5.7}$$

con $x \in M_d(\mathbb{Z}_p)$. La solución es por aproximación sucesiva. Comenzamos con $(1 + p^{n-1}a)^p \equiv 1 + p^n a (\mathrm{mod}\, p^{n+1})$ (siempre que n esté en el lugar indicado). Hagamos $x_1 = a$ y supongamos inductivamente que encontramos para $r \geq 1$, una matriz x_r conmutando con a, tal que $(1 + p^{n-1}x_r)^p \equiv 1 + p^n a (\mathrm{mod}\, p^{n+r})$. Digamos

$$(1 + p^{n-1}x_r)^p = 1 + p^n a + p^{n+r}c.$$

Ahora sea

$$z = (1 + p^{n-1}x_r)^{-(p-1)}c,$$

y sea $x_{r+1} = x_r - p^r z$; note que x_r conmuta con c, por tanto conmuta con z y así x_{r+1} conmuta con a. Un cálculo directo muestra que

$$(1 + p^{n-1}x_{r+1})^p \equiv 1 + p^n a \pmod{p^{n+r+1}}.$$

Así obtenemos una sucesión convergente (x_r) en $M_d(\mathbb{Z}_p)$, cuyo límite x satisface (5,7). □

Teorema. *Para cada i sea $\Gamma_i = \{\gamma \in \mathrm{GL}_d(\mathbb{Z}_p) \mid \gamma \equiv 1_d (\mathrm{mod}\, p^i)\}$. Definamos $G = \Gamma_1$ si p es impar, $G = \Gamma_2$ si $p = 2$. Entonces G es un grupo pro-p uniforme y $\dim(G) = \mathrm{rk}(G) = \mathrm{d}(G) = d^2$. También $P_i(G) = \Gamma_{i+\epsilon}$ para todo i, donde $\epsilon = 0$ si $p \neq 2$, $\epsilon = 1$ si $p = 2$.*

Demostración. Tenemos $P_1(G) = G = \Gamma_{1+\epsilon}$ por definición. Supongamos que $r \geq 1$ y $P_r(G) = \Gamma_{r+\epsilon}$. Entonces un cálculo fácil muestra que $P_r(G)^p[P_r(G), G] \leq \Gamma_{r+1+\epsilon}$ y por el Lema 3.2.1 mostramos que $\Gamma_{r+1+\epsilon} \leq \Gamma_{r+\epsilon}^p = P_r(G)^p$. Como $\Gamma_{r+1+\epsilon}$ es un subgrupo cerrado de G, tenemos que $P_{r+1}(G) = \Gamma_{r+1+\epsilon}$. Así por inducción sigue que $P_i(G) = \Gamma_{i+\epsilon}$ para todo i, y en el camino mostramos que $P_{i+1}(G) = P_i(G)^p$ para todo i. Tomando $i = 1$, vemos que G es powerful (cuando $p = 2$ notamos que $[\Gamma_2, \Gamma_2] \leq \Gamma_4 \leq \Gamma_2^4$); y como $P_2(G) = \Gamma_{2+\epsilon}$ es abierto en G, el Teorema 3.1.14 muestra que G es finitamente generado. Como $|\Gamma_i : \Gamma_{i+1}| = p^{d^2}$ es constante para

todo $i \geq 1$, G es uniforme. Finalmente, como $G/\Phi(G) = \Gamma_{1+\epsilon}/\Gamma_{2+\epsilon}$ es abeliano elemental de orden p^{d^2}, este tiene necesariamente d^2 generadores, de donde sigue que $\dim(G)$=rk(G)=d$(G) = d^2$. □

La teoría de los grupos powerful muestra que $\mathrm{GL}_d(\mathbb{Z}_p)$ tiene rango finito sin la necesidad de hacer cálculo pesado de matrices. Si conseguimos mostrar que cada grupo pro-p de rango finito tenga una representación lineal fiel sobre $\mathbb{Z}_p$, entonces esto proporcionará una caracterización más para los grupos pro-p de rango finito.

Teorema. *Un grupo pro-p es analítico p-ádico si y solo si es un subgrupo cerrado de $GL_d(\mathbb{Z}_p)$ para algún entero positivo d.*

5.7. Álgebras de Lie

Un álgebra de Lie es la estructura algebraica definida sobre un espacio vectorial, asociada usualmente a los grupos de Lie y usadas en el estudio geométrico de esos los propios grupos y de otras variedades diferenciables. El término "álgebra de Lie"(referido a Sophus Lie) fue creado por Hermann Weyl en la década de 1930, para lo que se denominaba "grupo infinitesimal".

Definición 5.7.1. Un *álgebra de Lie* $\mathfrak{a}$ es un espacio vectorial sobre un cuerpo F, junto con una operación binaria $[\cdot,\cdot] : \mathfrak{a} \times \mathfrak{a} \to \mathfrak{a}$, llamada *corchete de Lie*, que satisface las siguientes propiedades:

(i) es bilineal, es decir, $[ax+by, z] = a[x, z]+b[y, z]$ y $[z, ax+by] = a[z, x]+b[z, y]$, para todo $a, b \in F$ y $x, y, z \in \mathfrak{a}$

(ii) satisface la identidad de Jacobi [1], es decir $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$, para todo $x, y, z \in \mathfrak{a}$

(iii) $[x, x] = 0$, para todo $x \in \mathfrak{a}$.

Ejemplos 5.7.2.

1. Cada espacio vectorial se convierte en un álgebra de Lie *abeliana* trivial si definimos el corchete de Lie como idénticamente cero

2. El espacio euclídeo $\mathbb{R}^3$ se convierte en un álgebra de Lie con el corchete de Lie dado por el producto vectorial

3. Si se da un álgebra asociativa [2] A con la multiplicación $*$, se puede dar un álgebra de Lie definiendo $[x, y] = x * y - y * x$. esta expresión se llama el *conmutador* de x y y

[1] la identidad de Jacobi es el nombre para la ecuación siguiente, nombrada en honor de Carl Gustav Jakob Jacobi:

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0; \quad \text{para todo } X, Y, Z.$$

[2] Un *álgebra asociativa* es un módulo que también permite la multiplicación de vectores de manera distributiva y asociativa.

4. Inversamente, puede ser demostrado que cada álgebra de Lie se puede sumergir en otra que surja de un álgebra asociativa de esa manera

5. Otro ejemplo importante viene de la topología diferencial: los campos vectoriales en una variedad diferenciable forman un álgebra de Lie de dimensión infinita. Estos campos vectoriales actúan como operadores diferenciales sobre las funciones diferenciables sobre la variedad. Dados dos campos vectoriales X y Y, el corchete de Lie $[X, Y]$ se define como:
$$[X, Y]f = (XY - YX)f$$
y puede comprobarse que este operador corresponde a un campo vectorial. Las generalizaciones adecuadas de la teoría de variedades al caso de dimensión infinita muestra que esta álgebra de Lie es la asociada (ver siguiente punto) al grupo de Lie de los difeomorfismos de la variedad.

6. En el caso de una variedad que sea un grupo de Lie G a su vez, un subespacio de los campos vectoriales queda inalterado por las transformaciones dadas por el propio grupo, en el sentido de que en cada punto g del mismo, el campo no es más que:
$$X(g) = dl_g(X(e))$$

7. Como ejemplo concreto, consideremos el grupo de Lie $SL(n, \mathbb{R})$ de todas las matrices $n \times n$ con valores reales y determinante 1. El espacio tangente en la matriz identidad se puede identificar con el espacio de todas las matrices reales $n \times n$ con traza 0 y la estructura de álgebra de Lie que viene del grupo de Lie coincide con el que surge del conmutador de la multiplicación de matrices.

Definición 5.7.3. Sean $\mathfrak{a}$ y $\mathfrak{b}$ dos álgebras de Lie sobre el mismo cuerpo F. Un homomorfismo $\varphi : \mathfrak{a} \to \mathfrak{b}$ entre dos álgebras de Lie es una aplicación F-lineal tal que
$$[\varphi(x), \varphi(y)] = \varphi([x, y]), \text{ para todo } x, y \in \mathfrak{a}.$$

La composición de tales homomorfismos es otra vez un homomorfismo, y las álgebras de Lie sobre el cuerpo F, junto con estos morfismos, forman una categoría. Si tal homomorfismo es biyectivo, se llama *isomorfismo*, y las dos álgebras de Lie $\mathfrak{a}$ y $\mathfrak{b}$ se llaman *isomorfas*

Una *subálgebra* del álgebra de Lie $\mathfrak{a}$ es un subespacio vectorial $\mathfrak{b}$ de $\mathfrak{a}$ tal que $[x, y] \in \mathfrak{b}$ para todo $x, y \in \mathfrak{b}$, i.e. $[\mathfrak{b}, \mathfrak{b}] \subseteq \mathfrak{b}$. Así, la subálgebra es también un álgebra de Lie.

Un ideal del álgebra de Lie $\mathfrak{a}$ es un subespacio vectorial I de $\mathfrak{a}$ tal que $[a, y] \in I$ para todas $a \in \mathfrak{a}$ y $y \in I$, i.e. $[\mathfrak{a}, I] \subseteq I$. Todos los ideales son subálgebras. Sea I un ideal de $\mathfrak{a}$, entonces el espacio cociente $\mathfrak{a}/I$ se convierte en un álgebra de Lie definiendo $[x+I, y+I] = [x, y]+I$, para todos $x, y \in \mathfrak{a}$. Los ideales son precisamente los núcleos de homomorfismos, y el teorema fundamental de homomorfismos es válido para las álgebras de Lie.

Definición 5.7.4. Un álgebra de Lie $\mathfrak{a}$ se dice *nilpotente* si la serie central descendente
$$\mathfrak{a} \supseteq [\mathfrak{a}, \mathfrak{a}] \supseteq [[\mathfrak{a}, \mathfrak{a}], \mathfrak{a}] \supseteq [[[\mathfrak{a}, \mathfrak{a}], \mathfrak{a}], \mathfrak{a}] \cdots$$
termina en 0.

Teorema 5.7.5. (Engel). *Un álgebra de Lie es nilpotente si y solo si para cada $x \in \mathfrak{a}$, la aplicación $ad(x) : \mathfrak{a} \to \mathfrak{a}$, definida por*

$$ad(x)(y) = [x, y]$$

es nilpotente.

Definición 5.7.6. Un álgebra de Lie $\mathfrak{a}$ se dice *soluble* si la serie derivada

$$\mathfrak{a} \supseteq [\mathfrak{a}, \mathfrak{a}] \supseteq [[\mathfrak{a}, \mathfrak{a}], [\mathfrak{a}, \mathfrak{a}]] \supseteq [[[\mathfrak{a}, \mathfrak{a}], [\mathfrak{a}, \mathfrak{a}]], [[\mathfrak{a}, \mathfrak{a}], [\mathfrak{a}, \mathfrak{a}]]] \supseteq \cdots$$

termina en 0.

Una subálgebra $\mathfrak{b}$ de un álgebra $\mathfrak{a}$ se dirá *subálgebra de Borel* si es soluble y maximal. Un álgebra de Lie $\mathfrak{a}$ se llama *semisimple* si el único ideal soluble de $\mathfrak{a}$ es trivial. Un álgebra de Lie es *simple* si no tiene ningún ideal no trivial. En particular, un álgebra de Lie simple es semi-simple, y más generalmente, las álgebras de Lie semi-simples son suma directa de simples.

Sea G un grupo pro-p uniforme. Recordemos que $G_n = P_n(G) = G^{p^{n-1}}$ para cada $n \geq 1$. Sean $x, y \in G$ y $n \in \mathbb{N}$. Entonces $[x^{p^n}, y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$. Así tiene sentido definir una nueva operación en la forma siguiente:

$$(x, y)_n = [x^{p^n}, y^{p^n}]^{p^{-2n}}.$$

Lema 5.7.7. *Si $n > 1$, $x, y \in G$ y $u, v \in G_n$, entonces*

$$(xu, yv)_n \equiv (x, y)_n \equiv (x, y)_{n-1} \pmod{G_{n+1}}$$

y para todo $m > n$

$$(x, y)_m \equiv (x, y)_n \pmod{G_{n+2}}.$$

Demostración. (Dixon et al, 1999: 75).

Definición 5.7.8. Para cada $x, y \in G$ definimos:

$$(x, y) = \lim_{n \to \infty} (x, y)_n. \tag{5.8}$$

Teorema 5.7.9. *Con la operación $(\ ,\ )$, el $\mathbb{Z}_p$-módulo $(G, +)$ se torna un álgebra de Lie sobre $\mathbb{Z}_p$.*

Proposición 5.7.10. *Sea H un subgrupo cerrado uniforme de G, y sea $N \lhd_c G$ tal que G/N es uniforme. Entonces:*

(i) La aplicación inclusión $H \to G$ es un monomorfismo de álgebras de Lie $(H, +, (\ ,\ )) \to (G, +, (\ ,\ ))$; en particular, H es una subálgebra del álgebra de Lie $(G, +, (\ ,\ ))$;

(ii) N es uniforme;

(iii) N es un ideal en la $\mathbb{Z}_p$-álgebra de Lie $(G, +, (,))$: y las clases aditivas de N en G son las mismas que las clases multiplicativas, así $(G/N, +, (,)) = (G, +, (,))/(N, +, (,))$; además, el epimorfismo natural $* : G \to G/N$ es un epimorfismo de $\mathbb{Z}_p$-álgebras de Lie de $(G, +, (,))$ para $(G/N, +, (,))$.

Demostración. (Dixon et al, 1999: 77).

Obervación 5.7.11. Con las operaciones definidas en (5.6) y (5.8) el grupo pro-p uniforme G se torna una $\mathbb{Z}_p$-álgebra de Lie. Denotando esta álgebra por $\mathbf{log}(G)$. Sea $f : U \to V$ un homomorfismo entre dos grupos pro-p uniformes. Entonces $\mathbf{log}(f) = f$ es un homomorfismo de $\mathbb{Z}_p$-álgebras de Lie. En particular la acción de conjugación hace de $\mathbf{log}(G)$ un G-módulo.

Lema 5.7.12. *Sea G un grupo pro-p uniforme y sean $i, j \in \mathbb{N}$ tales que $i \leq j \leq 2i + 1$. Entonces G^{p^i}/G^{p^j} es abeliano y tenemos que*

$$G^{p^i}/G^{p^j} \cong \mathbf{log}(G)/p^{j-i}\mathbf{log}(G)$$

como G-módulos, donde G actúa por conjugación sobre G^{p^i}/G^{p^j}.

Demostración. Por la Proposición 5.2.7 (ii) tenemos que $[P_i(G), P_j(G)] \leq P_{i+j}(G)$ para todo i y j. Entonces de esto tenemos que $[P_{i+1}(G), P_{i+1}(G)] \leq P_{2i+2}(G)$. Luego obtenemos $[G^{p^i}, G^{p^i}] \leq G^{p^{2i+1}}$ y así $[G^{p^i}, G^{p^i}] \leq G^{p^{2i+1}} \leq G^{p^{2i}} \leq \cdots \leq G^{p^i}$. Resulta de esto que $[G^{p^i}, G^{p^i}] \leq G^{p^j}$, donde $i \leq j \leq 2i + 1$. Así obtenemos que G^{p^i}/G^{p^j} es abeliano para $i \leq j \leq 2i + 1$.

Para la otra parte. Por el Lema 5.6.13 (iii), $G_n = G^{p^{n-1}} = p^{n-1}\mathbf{log}(G)$. Luego tenemos que $G^{p^i}/G^{p^j} = p^i\mathbf{log}(G)/p^j\mathbf{log}(G) \cong \mathbf{log}(G)/p^{j-i}\mathbf{log}(G)$. □

Capítulo 6

Grupos analítico p-ádicos y teoría de Lie

En este capítulo, lidiamos con algunos resultados de los grupos analíticos p-ádicos y de la teoría de Lie, básicamente, para establecer un isomorfismo entre las categorías de grupos pro-p uniformes y las álgebras de Lie en $\mathbb{Z}_p$, también mostraremos una biyección entre la categoría de grupos analíticos p-ádicos y álgebras de Lie en $\mathbb{Q}_p$, tales biyecciones, mantienen la dimensión de los objetos, que es fundamental para la demostración del Teorema de González-Jaikin desarrollado en el capítulo 9. Las teorías de grupos analíticos p-ádicos y de Lie, así como las respectivas demostraciones pueden ser encontradas en 'Analytic Pro-p Groups' 2nd edn. de Dixon, J., Sautoy, M. du., Mann, A., Segal, D. (1999,pp: 178-235), que ha sido nuestra fuente para el desarrollo de este capítulo.

6.1. Variedades analíticas p-ádicas

Para $\mathbf{y} \in \mathbb{Z}_p^r$ y $h \in \mathbb{N}$ definimos

$$\begin{aligned} B(\mathbf{y}, p^{-h}) &= \{\mathbf{z} \in \mathbb{Z}_p^r \mid |z_i - y_i| \leq p^{-h}, \forall i = 1, \cdots, r\} \\ &= \{\mathbf{y} + p^h\mathbf{x} \mid \mathbf{x} \in \mathbb{Z}_p^r\}. \end{aligned}$$

Definición 6.1.1. Sea V un subconjunto abierto no vacío de $\mathbb{Z}_p^r$ y sea

$$\mathbf{f} = (f_1, \cdots, f_s)$$

una función de V en $\mathbb{Z}_p^s$.

(i) Sea $\mathbf{y} \in V$. Entonces $\mathbf{f}$ es *analítica* en $\mathbf{y}$ si existe $h \in \mathbb{N}$ con $B(\mathbf{y}, p^{-h}) \subseteq V$ y una serie formal de potencias $F_i(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ $(i = 1, \cdots, s)$ tal que $f_i(\mathbf{y} + p^h\mathbf{x}) = F_i(\mathbf{x})$ para todo $\mathbf{x} \in \mathbb{Z}_p^r$

(ii) La función $\mathbf{f}$ es *analítica sobre* V si es analítica en cada punto de V.

Lema 6.1.2. *Supongamos que $F(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ puede ser evaluado en $\mathbf{x}$ para todo $\mathbf{x} \in \mathbb{Z}_p^r$. Sea $\mathbf{a} \in \mathbb{Z}_p^r$. Entonces existe $G(\mathbf{X}) \in \mathbb{Q}_p[[\mathbf{X}]]$ tal que $F(\mathbf{x} + \mathbf{a}) = G(\mathbf{x})$ para todo $\mathbf{x} \in \mathbb{Z}_p^r$.*

Corolario 6.1.3. *Supongamos que $V \subseteq \mathbb{Z}_p^r$ puede ser escrito como una unión*

$$\bigcup \{B(\mathbf{y}(i), p^{-h(i)}) \mid i \in I\}$$

de bolas y que $\mathbf{f} = (f_1, ..., f_s)$ *es una función de* V *en* $\mathbb{Z}_p^s$ *tal que, para cada* $i \in I$*, las funciones* $\mathbf{x} \to f_j(\mathbf{y}(i) + p^{h(i)}\mathbf{x})$ *son estrictamente analíticas sobre* $\mathbb{Z}_p^r$ *para* $j = 1, ..., s$*. Entonces* $\mathbf{f}$ *es analítica sobre* V*.*

Lema 6.1.4. *Sean* $\mathbf{f} : U \to V$ *y* $\mathbf{g} : V \to W$ *dos funciones analíticas, donde* $U \subseteq \mathbb{Z}_p^r$*,* $V \subseteq \mathbb{Z}_p^s$ *y* $W \subseteq \mathbb{Z}_p^t$ *son conjuntos abiertos no vacíos. Entonces* $\mathbf{g} \circ \mathbf{f}$ *es analítica sobre* V*.*

Definición 6.1.5. (i) Sea X un espacio topológico y U un subconjunto abierto no vacío de X. Una terna (U, ϕ, n) es una *carta* sobre X si ϕ es un homeomorfismo de U sobre un subconjunto abierto de $\mathbb{Z}_p^n$ para algún $n \in \mathbb{N}$. La *dimensión* de la carta es n. La carta (U, ϕ, n) es una *carta global* si $U = X$,

(ii) Dos cartas (U, ϕ, n) y (V, ψ, m) sobre un espacio topológico X son *compatibles* si las aplicaciones $\psi \circ \phi^{-1}|_{\phi(U \cap V)}$ y $\phi \circ \psi^{-1}|_{\psi(U \cap V)}$ son funciones analíticas sobre $\phi(U \cap V)$ y $\psi(U \cap V)$ respectivamente,

(iii) Un *atlas* sobre un espacio topológico X es un conjunto de pares compatibles de cartas que cubren X, i.e. es un conjunto de la forma

$$A = \{(U_i, \phi_i, n_i) \mid i \in I\}$$

con las siguientes propiedades

- Para cada $i \in I$, (U_i, ϕ_i, n_i) es una carta sobre X
- para cada $i, j \in I$, (U_i, ϕ_i, n_i) y (U_j, ϕ_j, n_j) son compatibles
- $X = \bigcup_{i \in I} U_i$.

A es un *atlas global* si para algún $i \in I$ la carta (U_i, ϕ_i, n_i) es global,

(iv) Sean A y B dos atlas sobre un espacio topológico X. Entonces A y B son *compatibles* si cada carta en A es compatible con cada carta en B; esto es, si $A \cup B$ es un atlas sobre X.

con X_A denotamos el espacio topológico dotado de un atlas A. Una función $f : X_A \to Y_B$ se dice *analítica* si para cada par de cartas $(U, \phi, n) \in A$ y $(V, \psi, m) \in B$, se satisface lo siguiente:

(i) $f^{-1}(V)$ es abierto en X y

(ii) la composición $\psi \circ f \circ \phi^{-1}|_{\phi(u \cap f^{-1}(V))}$ es una función analítica del conjunto abierto $\phi(U \cap f^{-1}(V)) \subseteq \mathbb{Z}_p^n$ en $\mathbb{Z}_p^m$.

Lema 6.1.6. *Sean* X, Y *y* Z *espacios topológicos y* A, B, C *atlas sobre* X, Y, Z *respectivamente. Si* $f : X_A \to Y_B$ *y* $g : Y_B \to Z_C$ *son analíticas, entonces* $g \circ f : X_A \to Z_C$ *es analítica.*

La compatibilidad es una relación de equivalencia sobre la clase de todos los atlas sobre X. Por tanto tenemos.

Definición 6.1.7. Sea X un espacio topológico. Una *estructura de variedad analítica p-ádica* sobre X es una clase de equivalencia de atlas compatibles sobre X. Si tal estructura

existe, X es una *variedad analítica p-ádica*. Cualquier atlas perteneciendo a esa clase de equivalencia es llamado un atlas de (la variedad) X; cualquier carta perteneciendo a este atlas es una carta de (la variedad) X.

De ahora en adelante, vamos a escribir "variedad analítica" o "variedad" en lugar de "variedad analítica p-ádica".

Ejemplos 6.1.8.

(i) Consideremos un espacio topológico discreto X. Entonces X puede considerarse una variedad analítica p-ádica con estructura determinada por $\{(\{x\}, \phi_x, 0) \mid x \in X\}$, donde $\phi_x : x \to 0$,

(ii) Sea $X = \mathbb{Q}_p^n$. Para cada $i \in \mathbb{N}$, sea $\phi_i : p^{-i}\mathbb{Z}_p^n \to \mathbb{Z}_p^n$ la aplicación definida por $\phi_i(x) = p^i x$. Entonces el conjunto $A = \{(p^{-i}\mathbb{Z}_p^n, \phi, n) \mid i \in \mathbb{N}\}$ es una atlas sobre X pues $\{(p^{-i}\mathbb{Z}_p^n \mid i \in \mathbb{N}\}$ es un cubrimiento abierto de $\mathbb{Q}_p^n$. Este atlas dota a X de una estructura de variedad analítica p-ádica,

(iii) Sea X un variedad y sea U un subconjutno abierto de X. Si $A = \{(V_i, \phi_i, n_i) \mid i \in I\}$ es un atlas de X. Entonces $B = \{(V_i \cap U, \phi_i|_{V_i \cap U}, n_i) \mid i \in I\}$ es un atlas sobre U y la estructura de variedad determinada por este atlas se llama *estructura de variedad inducida* sobre U. Si M y N son variedades analíticas p-ádicas tal que M es un subconjunto abierto de N y la estructura de variedad sobre M es una estructura de variedad inducida por N, entonces decimos que N *extiende* la estructura de variedad sobre N,

(iv) Sean X y Y variedades analíticas determinadas por los atlas A y B respectivamente. Entonces $Z = X \times Y$ tiene estructura de variedad analítica definida por el atlas $C = \{(U \times V, \phi \times \psi, m + n) \mid (U, \phi, m) \in A, (V, \psi, n) \in B\}$, donde la aplicación $\phi \times \psi : U \times V \to \mathbb{Z}_p^{m+n}$ es definida como $(\phi \times \psi)(u, v) = ((u), \psi(v))$. Llamemos a esta variedad, el *producto* de X y Y.

Definición 6.1.9. Sean X y Y variedades analíticas y $f : X \to Y$ una función, f es *analítica* si existen dos atlas A y B de X y Y respectivamente tal que $f : X_A \to Y_B$ es analítica.

Lema 6.1.10. *Supongamos que $f : X \to Y$ y $g : Y \to Z$ son funciones analíticas donde X, Y y Z son variedades analíticas. Entonces $g \circ f : X \to Z$ es una función analítica.*

Lema 6.1.11. *Sea $f : X \to Y$ una función, donde X y Y son variedades. Supongamos que $X = \bigcup_{i \in I} X_i$ tal que los X_i son subconjuntos abiertos en X y que $f|_{X_i} : X_i \to Y$ son analíticas en relación a la estructura de variedad inducida sobre X_i, para cada $i \in I$. Entonces f es una función analítica.*

Lema 6.1.12. *Sea $f : X \to Y$ una función analítica. Entonces f es continua.*

6.2. Grupos analíticos p-ádicos

En esta sección definiremos lo que son grupos analítico p-ádicos y daremos algunas propiedades de estos.

Definición 6.2.1. Un grupo topológico G es un *grupo analítico p-ádico* si G tiene una estructura de variedad analítica p-ádica con las propiedades

(i) La función $f : G \times G \to G$ dada por $(x, y) \mapsto xy$ es analítica.

(ii) La función $i : G \to G$ definida por $x \mapsto x^{-1}$ es analítica.

Proposición 6.2.2. *Sea G un grupo topológico conteniendo un subgrupo abierto H. Supongamos que H tiene estructura de grupo analítico p-ádico, y que: para cada $g \in G$, existe una vecindad abierta V_g de la identidad en H tal que*

(i) $gVgg^{-1} \subseteq H$ *y*

(ii) *la función $k_g : V_g \to H$ definida por $x \mapsto gxg^{-1}$ es analítica.*

Entonces existe una única estructura de variedad analítica sobre G extendiendo la estructura de variedad sobre H y tornándose G un grupo analítico p-ádico.

Lema 6.2.3. *Sean G y G' dos grupos analíticos p-ádicos y sea $\phi : G \to G'$ un homomorfismo de grupos. Supongamos que $\phi|_H$ es analítica para un subgrupo abierto H de G. Entonces ϕ es una función analítica.*

Ejemplos 6.2.4.

(i) Sea G un grupo dotado con la topología discreta y estructura de variedad definida por $\{(\{x\}, \phi_x, 0) \mid x \in X\}$, donde $\phi_x : x \to 0$. Como cualquier aplicación sobre tal variedad es analítica, G sería un grupo analítico p-ádico,

(ii) Consideremos el grupo $\mathbb{Q}_p^n$ con la operación de adición y estructura de variedad analítica definida por el Ejemplo 6.1.8 (ii), la función definida como $(x, y) \mapsto x - y$ es analítica. Así, G es un grupo analítico p-ádico,

(iii) Sea G un grupo analítico p-ádico y sea H un subgruo abierto de G. Entonces considerando la estructura de variedad analítica definida inducida de G (Ejemplo 6.1.8 (iii)), H sería un grupo analítico p-ádico,

(iv) El grupo $G = GL_n(\mathbb{Q}_p^n)$, también tiene estructura de grupo analítico p-ádico (Proposición 6.2.2).

El siguiente resultado se ubica dentro de los grupos pro-p uniformes

Teorema 6.2.5. *Sea G un grupo topológico conteniendo un subgrupo abierto que es un grupo pro-p uniforme. Entonces G es un grupo analítico p-ádico.*

6.3. Grupos estándar

En esta sección vamos a mostrar el inverso del Teorema 6.2.5.

Sean $X_1, X_2, \cdots, Y_1.Y_2, \cdots$ indeterminadas, entonces el siguiente

$$\mathbb{Z}_p[[X_1, ..., X_n]] = \mathbb{Z}_p[[\mathbf{X}]]$$

denota el subanillo de $\mathbb{Q}_p[[\mathbf{X}]]$ consistente de las series formales de potencias

$$F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha X_1^{\alpha_1} ... X_n^{\alpha_n} = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \mathbf{X}^\alpha$$

donde $a_\alpha \in \mathbb{Z}_p$ para cada $\alpha \in \mathbb{N}^n$. Notamos que $F(\mathbf{X}) \in \mathbb{Z}_p[[\mathbf{X}]]$ entonces $F(\mathbf{X})$ existe para todo $\mathbf{x} \in p\mathbb{Z}_p^n$.

Definición 6.3.1. Sea G un grupo analítico p-ádico. Entonces G es un *grupo estándar* (de dimensión r sobre $\mathbb{Q}_p$) si

(i) la estructura de variedad analítica sobre G es definida por un atlas global de la forma $\{(G, \psi, r)\}$ donde ψ es un homeomorfismo de G sobre $p\mathbb{Z}_p^r$ (si $p > 2$) o sobre $4\mathbb{Z}_2^r$ (si $p = 2$), con $\psi(1) = 0$, y

(ii) para $j = 1, \cdots, r$ existe $P_j(\mathbf{X}, \mathbf{Y}) \in \mathbb{Z}_p[[\mathbf{X}, \mathbf{Y}]]$ tal que

$$\psi_j(xy^{-1}) = P_j(\psi(x), \psi(y))$$

para todo $x, y \in G$, donde $\psi = (\psi_1, \cdots, \psi_r)$

Lema 6.3.2. *Sea $G[Y_1, \cdots, Y_m] \in \mathbb{Z}_p[\mathbf{Y}]$ y sean $F_i[\mathbf{X}] \in \mathbb{Z}_p[\mathbf{X}]$ para $i = 1, \cdots, m$. Supongamos que cada una de las series $F_i[\mathbf{X}]$ tenga término constante 0. Entonces $G \circ \mathbf{F} \in \mathbb{Z}_p[\mathbf{X}]$ y $(G \circ \mathbf{F})(\mathbf{x}) = G(F_1(\mathbf{x}), \cdots, F_m(x))$ para todo $\mathbf{x} \in p\mathbb{Z}_p^m$.*

Lema 6.3.3. *Sea G un grupo estándar de dimensión r. Sea $\omega(x_1, \cdots, x_n)$ una palabra del grupo en las variables $x_1, \cdots, x_n$. Entonces existe*

$$F_j[X_{11}, \cdots, X_{1r}, \cdots, X_{n1}, \cdots, X_{nr}] \in \mathbb{Z}_p[[\mathbf{X}_1, \cdots, \mathbf{X}_n]]$$

$(j = 1, \cdots, r)$ tal que para todo $x_1, \cdots, x_n \in G$

$$\psi_j(\omega(x_1, \cdots, x_n)) = F_j(\psi(x_1), \cdots, \psi(x_n))$$

Lema 6.3.4. *Sea $F(\mathbf{X}) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \mathbf{X}^\alpha \in \mathbb{Q}_p[[\mathbf{X}]]$. Supongamos que existe una vecindad abierta V de 0 en $\mathbb{Q}_p$ tal que, para todos $\lambda_1, \cdots, \lambda_n \in V^n$,*

$$F(\lambda_1, \cdots, \lambda_n) = 0$$

Entonces $a_\alpha = 0$ para todo $\alpha \in \mathbb{N}^n$.

Ahora estamos listos para mostrar el primer resultado de esta sección.

Teorema 6.3.5. *Sea G un grupo analítico p-ádico. Entonces G tiene un subgrupo abierto H que es un grupo estándar en relación a la estructura de variedad inducida por G.*

Precisamos de un Lema más, antes de completar la prueba del resultado principal.

Lema 6.3.6. *Sea G un grupo estándar sobre $\mathbb{Q}_p$ con un atlas global $\{(G, \psi, r)\}$. Entonces existen series de potencias $F_1(\mathbf{X}), \cdots, F_r(\mathbf{X}) \in \mathbb{Z}_p[[\mathbf{X}_1, \cdots, \mathbf{X}_r]]$ tal que*

$$\begin{aligned} \psi(x^p) &= F(\psi(x)) \text{ para todo } x \in G \\ F_k(\mathbf{X}) &= pX_k + \sum_{\langle \alpha \rangle > 1} c_{k,\alpha} \mathbf{X}^\alpha \text{ para cada } k, \end{aligned}$$

donde $c_{k,\alpha} \in \mathbb{Z}_p$ *para cada* α *y* k. *También cada* $c_{k,\alpha} \equiv 0(\ \text{mód}\ p)$ *donde* $\langle\alpha\rangle = 2$, *siempre que* $p \neq 2$.

Teorema 6.3.7. *Sea* G *un grupo estándar de dimensión* r *sobre* $\mathbb{Q}_p$. *Entonces* G *es un grupo pro-p uniforme de dimensión* r.

Teorema 6.3.8. *Sea* G *un grupo topológico. Entonces* G *tiene estructura de un grupo analítico p-ádico si y solo si* G *contiene un subgrupo abierto que es un grupo pro-p uniforme.*

Corolario 6.3.9. *Un grupo topológico* G *es analítico p-ádico si y solo si* G *tiene un subgrupo abierto que es un grupo pro-p de rango finito.*

Corolario 6.3.10. *Las siguientes son equivalentes para un grupo topológico* G*:*

(i) G *es un grupo compacto analítico p-ádico,*

(ii) G *contiene un subgrupo abierto normal pro-p uniforme de índice finito,*

(iii) G *es un grupo profinito conteniendo un subgrupo abierto que es un grupo pro-p de rango finito.*

Corolario 6.3.11. *Sea* G *un grupo compacto analítico p-ádico. Entonces* $\mathrm{Aut}(G)$ *es un grupo compacto analítico p-ádico.*

Definamos la *dimensión* para un grupo analítico p-ádico.

Teorema 6.3.12. *Sea* G *un grupo analítico p-ádico. Entonces existe un único entero no negativo* n *con las siguientes propiedades:*

- *cada carta perteneciendo a un atlas definiendo la estructura de variedad sobre* G *tiene dimensión* n, *en el sentido de la Definición 6.1.5,*
- *cada subgrupo abierto pro-p de* G *tiene rango finito y dimensión* n, *en el sentido de la Definición 6.6.7.*

Definición 6.3.13. Sea G un grupo analítico p-ádico. Entonces la *dimensión*

$$\dim(G)$$

de G es el número n especificado en el Teorema 6.3.12.

6.4. Teoría de Lie

A continuación presentamos algunos resultados dentro de la teoría de Lie.

Lema 6.4.1. *Sea* G *un grupo estándar en relación a la carta global* (G, ψ, d). *Sea* $G_2 = P_2(G)$, *y sea* $\{u_1, \cdots, u_d\}$ *un conjunto de generadores topológicos para* G, *definamos* $\phi : G \to \mathbb{Z}_p^d$ *por* $\phi(u_1^{\lambda_1}, \cdots, u_d^{\lambda_d}) = \lambda$ *para cada* $\lambda = (\lambda_1, \cdots, \lambda_d) \in \mathbb{Z}_p^d$ *Entonces las cartas* $(G, \psi|_{G_2}, d)$ *y* $(G, \phi|_{G_2}, d)$ *son compatibles.*

Un resultado importante es el siguiente.

Teorema 6.4.2. *Sean G_1 y G_2 grupos analítico p-ádicos . Entonces cada homomorfismo continuo $G_1 \to G_2$ es analítico.*

Corolario 6.4.3. *Sea G un grupo topológico. Entonces G tiene como máximo una estructura de grupo analítico p-ádico; y a menos que G sea discreto, el primo p es unicamente determinado.*

Teorema 6.4.4. *Sea G un grupo analítico p-ádico. Sean H un subgrupo cerrado de G y N un subgrupo normal cerrado de G.Entonces*

(i) *H es analítico p-ádico, y la aplicación inclusión $H \to G$ es un homomorfismo analítico,*

(ii) *G/N con la topología cociente es analítico p-ádico, y la proyección natural $G \to G/N$ es un homomorfismo analítico.*

Teorema 6.4.5. *Sea G un grupo topológico Hausdorff, y N un subgrupo normal cerrado. Si ambos N y G/N son analítico p-ádicos (con la topología inducida y cociente respectivamente), entonces G es analítico p-ádico.*

6.5. Álgebras de Lie powerful

En su libro Dixon abre esta sección de la siguiente manera: En esta sección vamos a mostrar como la correspondencia que atribuye un álgebra de Lie a cada grupo pro-p uniforme puede ser invertida.

Fijemos

$$\epsilon = 1 \text{ si } p \text{ es impar, } \epsilon = 2 \text{ si } p = 2$$

Un álgebra de Lie L sobre $\mathbb{Z}_p$ es llamada *powerful* si $L \cong \mathbb{Z}_p^d$ para algún entero positivo d y

$$(L, L) \subseteq p^{\epsilon} L.$$

La fórmula siguiente es llamada la *fórmula de Campbell-Hausdorff*

$$\begin{aligned} \Phi(X,Y) &= \sum_{n=1}^{\infty} u_n(X,Y) \\ u_1(X,Y) &= X + Y, \;\; u_2 = \frac{1}{2}(X,Y) \\ u_n(X,Y) &= \sum_{\mathbf{e}} q_{\mathbf{e}} (X,Y)_{\mathbf{e}} \;\; (n \geq 3) \end{aligned} \tag{6.1}$$

donde $(X,Y)_{\mathbf{e}} = (X, Y, \cdots, Y, X, \cdots, X, \cdots)$ denota un corchete de Lie a izquierda-normado de longitud $\langle \mathbf{e} \rangle + 1$, y la suma en (5.1) es sobre los vectores $\mathbf{e}$ de enteros positivos satisfaciendo $\langle \mathbf{e} \rangle = n - 1$. Los coeficientes $q_{\mathbf{e}}$ son números racionales satisfaciendo

$$p^{\epsilon \langle \mathbf{e} \rangle} q_{\mathbf{e}} \in p^{\epsilon} \mathbb{Z}_p, \; |p^{\epsilon \langle \mathbf{e} \rangle} q_{\mathbf{e}}| \longrightarrow 0 \text{ cuando } \langle \mathbf{e} \rangle \longrightarrow \infty$$

Como cada $u_n(X,Y)$ es una suma finita, podemos evaluar en cualquier álgebra de Lie sobre $\mathbb{Q}_p$; L es una $\mathbb{Z}_p$-álgebra de Lie *powerful*, entonces de hecho $u_n(X,Y)$ puede ser evaluado en L, y para $x, y \in L$ la serie

$$\tilde{\Phi}(X,Y) = \sum_{n=1}^{\infty} u_n(X,Y)$$

converge en L. podemos por tanto definir una operación binaria $* : L \times L \to L$ por

$$x * y = \tilde{\Phi}(x,y)$$

(Dixon et al, 1999: 221).

Teorema 6.5.1. *Sea L un álgebra de Lie powerful. Entonces la operación $*$ hace de L un grupo pro-p uniforme. Si $\{a_1, ..., a_d\}$ es una base para L sobre $\mathbb{Z}_p$ entonces $\{a_1, ..., a_d\}$ es un conjunto de generadores topológicos para el grupo $(L, *)$, y tiene dimensión d.*

Lema 6.5.2. *La operación $*$ sobre un álgebra de Lie powerful es asociativa.*

Teorema 6.5.3. *Las aplicaciones*

$$G \mapsto L_G,\ L \mapsto (L, *)$$

son mutuamente isomorfismos inversos entre la categoría de grupos pro-p uniformes y la categoría de álgebras de Lie powerful sobre $\mathbb{Z}_p$.

Consideremos el grupo analítico p-ádico G. Por el Teorema 6.3.8, G tiene un subgrupo que es un grupo pro-p uniforme. Si H_1 y H_2 son ambos subgrupos abiertos uniformes de G, entonces $H = H_1 \cap H_2$ tiene índice finito en H_1 y H_2, así L_H tiene índice finito en L_{H_i} para $i = 1, 2$. Por tanto

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_1} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_{H_2}.$$

Podemos por tanto inequívocamente definir

$$\mathcal{L}(G) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_H \tag{6.2}$$

donde H es cualquier subgrupo abierto uniforme de G. Por tanto tenemos

$$\begin{array}{rcll} \dim_{\mathbb{Q}_p}\mathcal{L}(G) & = & \dim_{\mathbb{Z}_p} L_H & \text{(por (6.2))} \\ & = & \mathrm{d}(H) & \text{(Teorema 6.5.1)} \\ & = & \dim(G) & \text{(Definición 5.6.7)} \end{array}$$

y así $\mathcal{L}(G)$ es el álgebra de Lie sobre $\mathbb{Q}_p$; de dimensión igual a $\dim(H)$=$\dim(G)$.

Ahora supongamos que $f : G_1 \to G_2$ es un morfismo de grupos analíticos. Escogemos un subgrupo abierto uniforme H_2 en G_2; como f es continuo, el subgrupo $f^{-1}(H_2)$ es abierto en G_1, por tanto contiene un subgrupo abierto uniforme H_1. El homomorfismo de grupos $f_0 = f|_{H_1} : H_1 \to H_2$ es al mismo tiempo un homomorfismo de álgebras de Lie de L_{H_1} para L_{H_2}, como observamos en el Teorema 6.5.3; y por tanto este induce un homomorfismo de álgebras de Lie

$$f^* = 1 \otimes f_0 : \mathcal{L}(G_1) \to \mathcal{L}(G_2);$$

Claramente f^* no depende de la elección de H_2 y H_1. También, si $f : G_1 \to G_2$ y $g : G_2 \to G_3$ son morfismos, entonces

$$(g \circ f)^* = g^* \circ f^*;$$

y $(Id_G)^* = Id_{\mathcal{G}}$ son morfismos. Así hemos demostrado la primera parte del siguiente teorema:

Teorema 6.5.4 (i) *La aplicación $G \mapsto \mathcal{L}(G)$, $f \to f^*$ es un functor de la categoría de grupos analítico p-ádicos (de dimensión d) para la categoría de álgebras de Lie sobre $\mathbb{Q}_p$ (de dimensión d),*

(ii) *Sean $f_1, f_2 : A \to B$ morfismos de grupos analítico p-ádicos . Entonces $f_1^* = f_2^* : \mathcal{L}(A) \to \mathcal{L}(B)$ si y solo si $f_1|_U = f_2|_U$ para algún subgrupo abierto U de A,*

(ii) *Sea G un grupo analítico p-ádico, identifiquemos $\mathcal{L}(G)$ con $\mathbb{Q}_p^d$ eligiendo una base. Entonces G tiene un subgrupo abierto uniforme H tal que la composición*

$$\phi : H \xrightarrow{Id} L_H \xrightarrow{1\otimes -} \mathcal{L}(G) = \mathbb{Q}_p^d$$

da una carta (H, ϕ, d) de G.

Capítulo 7

Cohomología de grupos profinitos

En este capítulo, abordaremos el concepto de cohomología de grupos profinitos y para este fin recurriremos a teoremas importantes obtenidos de J. Neukirch, A. Schmidt and K. Wingberg, "Cohomology of Number Fields"(2008) y J. S. Wilson, "Profinite Groups"(1997). El resultado más importante de este capítulo es el Lemma 7.3.6 que afirma que a partir de una sucesión exacta corta, obtenemos una sucesión exacta larga de grupos de cohomología de un grupo profinito G sobre G-módulos topológicos.

7.1. Cohomología de Grupos

Sea G un grupo. Un *G-módulo a derecha* es un grupo abeliano A junto con una aplicación $\sigma : A \times G \to A$. Escribamos $\sigma(a, g) = ag$. Esta aplicación tiene que satisfacer las siguientes condiciones.

(i) $(a_1 + a_2)g = a_1g + a_2g$, para todos $a_1, a_2 \in A$ y para todo $g \in G$

(ii) $a(g_1g_2) = (ag_1)g_2$, para todo $a \in A$ y todos los $g_1, g_2 \in G$

(iii) $a1 = a$, para todo $a \in A$.

Un *G-módulo a izquierda* es definido de forma análoga. Cualquier G-módulo a izquierda puede ser visto como un G-módulo a derecha definiendo $ag = g^{-1}a$, para todo $a \in A$ y $g \in G$. A partir de ahora solamente usaremos G-módulos a derecha. Entonces no vamos a considerar la palabra *derecha* y solamente lo llamaremos un *G-módulo*. Diremos que A es un *G-módulo topológico* si la aplicación σ es continua.

Definición 7.1.1. Sea G un grupo profinito. Para cada G-módulo topológico A y cada subgrupo H de G escribimos

$$A^H = \{a \mid ah = a \text{ para todo } h \in H\}$$

Definición 7.1.2. Sea G un grupo profinito y A un G-módulo topológico. Para cada $n \in \mathbb{N}$ y $n > 0$ definimos el conjunto

$$C^n(G, A) = \{f \mid f : G^n \to A \text{ es una aplicación continua}\}.$$

Definición 7.1.3. Sea G un grupo profinito y A un G-módulo topológico. Para cada $n \in \mathbb{N}$ y $n > 0$ definimos la aplicación $\partial_n : C^{n-1}(G, A) \to C^n(G, A)$ dada por

$$(\partial_n f)(x_1, ..., x_n) = f(x_2, ..., x_n) + \sum_{i=1}^{n-1} (-1)^i f(x_1, ..., x_i x_{i+1}, ..., x_n) + (-1)^n f(x_1, ..., x_{n-1}) x_n$$

- Si $n = 0$, entonces $G^{(0)} = 1$.
- $C^0(G, A) = A$.
- $\partial_1 : C^0(G, A) \to C^1(G, A)$ es la aplicación $(\partial_1 a)x = a - ax$
- $\partial_0 : 0 \to C^0(G, A)$ es la aplicación $\partial_0 \equiv 0$.

Lema 7.1.4. *$\partial_{n+1}\partial_n$ es la aplicación 0 de $C^{n-1}(G, A)$ para $C^{n+1}(G, A)$, para cada $n > 0$.*

Definimos

$$B^n(G, A) = \text{im } \partial_n \qquad \text{y} \qquad Z^n(G, A) = \ker \partial_{n+1}.$$

Podemos mostrar por inducción sobre n que $B^n(G, A) \lhd Z^n(G, A)$. Así tenemos la siguiente definición.

Definición 7.1.5. Sea G un grupo profinito y A un G-módulo topológico. Entonces $H^n(G, A) = Z^n(G, A)/B^n(G, A)$ es el *n-ésimo grupo de cohomología de G* con coeficientes en el módulo A.
Si $n = 0$, tenemos

$$\begin{aligned} H^0(G, A) &= \frac{Z^0(G, A)}{B^0(G, A)} = \frac{Z^0(G, A)}{\{0\}} \cong Z^0(G, A) = \{a \in A \mid \partial_1 a = 0\} \\ &= \{a \in A \mid x \mapsto a - ax \text{ es la aplicación 0 sobre } G\} \\ &= A^G. \end{aligned}$$

Sea p un primo y G un grupo profinito. El *subgrupo p-Frattini* $\Phi_p(G)$ de G es la cerradura del subgrupo abstracto generado por el conjunto

$$\{x^{-1}y^{-1}xy \mid x, y \in G\} \cup \{x^p \mid x \in G\}.$$

Lema 7.1.6. *Sea G un grupo profinito. Entonces $H^1(G, A) = \text{Hom}(G, A)$ para cada G-módulo topológico A sobre el cual G actúa trivialmente, y*

$$H^1(G, \mathbb{F}_p) = \text{Hom}(G/\Phi_p(G), \mathbb{F}_p)$$

donde $\mathbb{F}_p$ es visto como un módulo sobre el cual G actúa trivialmente.

7.2. Pares compatibles de aplicaciones

Definamos lo que significa un *par compatible.*

Definiciones 7.2.1. Sea $\theta : G_1 \to G_2$ un homomorfismo continuo de grupos profinitos, sean A_i unos G_i-módulos para cada $i = 1, 2$ y $\varphi : A_2 \to A_1$ un homomorfismo continuo de grupos topológicos abelianos. El par (θ, φ) es llamado *compatible* si para todo $x \in G_1$ y $a \in A_2$ tenemos $\varphi(a\theta(x)) = \varphi(a)x$.

Lema 7.2.2. *Sean $\theta : G_1 \to G_2$ y $\varphi : A_2 \to A_1$ un par compatible.*

(a) *Para cada $n \geq 0$ existe un homomorfismo inducido*

$$(\theta, \varphi)^* : C^n(G_2, A_2) \to C^n(G_1, A_1)$$

definido por $((\theta, \varphi)^* f) = \varphi f(\theta x_1, \cdots, \theta x_n)$

(b) *El diagrama*

$$\begin{array}{ccc} C^n(G_2, A_2) & \xrightarrow{\partial} & C^{n+1}(G_2, A_2) \\ \downarrow & & \downarrow \\ C^n(G_1, A_1) & \xrightarrow{\partial} & C^{n+1}(G_1, A_1) \end{array}$$

con las aplicaciones verticales $(\theta, \varphi)^*$ es conmutativa para cada $n \geq 0$

(c) *Para cada $n \geq 0$ existe una aplicación inducida $H^n(G_2, A_2) \to H^n(G_1, A_1)$ definida por $f + B^n(G_2, A_2) \mapsto (\theta, \varphi)^* f + B^n(G_1, A_1)$ (esta aplicación también es denotada por $(\theta, \varphi)^*$).*

Lema 7.2.3.

(a) *Si θ, φ son aplicaciones identidades, entonces $(\theta, \varphi)^*$ es la aplicación identidad*

(b) *Si $G_1 \xrightarrow{\theta_1} G_2 \xrightarrow{\theta_2} G_3$ y $A_3 \xrightarrow{\varphi_2} A_2 \xrightarrow{\varphi_1} A_1$ son tales que las aplicaciones (θ_1, φ_1) y (θ_2, φ_2) son compatibles, entonces la aplicación inducida satisface $(\theta_2\theta_1, \varphi_1\varphi_2)^* = (\theta_1, \varphi_1)^*(\theta_2, \varphi_2)^*$.*

7.3. La sucesión exacta larga

Sea G un grupo profinito y sean A y B dos G-módulos. Para cada aplicación $\varphi : A \to B$ existe un homomorfismo $\varphi_n : H^n(G, A) \to H^n(G, B)$ definido por $f + B^n(G, A) \mapsto \varphi f + B^n(G, B)$. Además, podemos ver que $H^n(G, -)$ es un functor covariante de la categoría de G-módulos para la categoría de grupos abelianos.

(i) Dado un homomorfismo de G-módulos $A \xrightarrow{i} B \xrightarrow{j} C$ tenemos $j_n i_n = (ji)_n$, y

(ii) si $\varphi : A \to A$ es la aplicación identidad entonces $\varphi_n : H^n(G, A) \to H^n(G, A)$ es la aplicación identidad.

Una *sucesión exacta* de grupos es una sucesión (finita o infinita)

$$\cdots \longrightarrow G_{n-1} \xrightarrow{f_{n-1}} G_n \xrightarrow{f_n} G_{n+1} \longrightarrow \cdots \tag{7.1}$$

de grupos y homomorfismos tales que $\ker f_n = \text{im } f_{n-1}$ para cada $n \geq 0$.

La sucesión en (7,1) se dice *exacta en* G_n *si* $\ker f_n = \text{im } f_{n-1}$.

Una *sucesión exacta corta* es una sucesión de la forma

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 1,$$

o equivalentemente es una sucesión exacta con la propiedad adicional que i es inyectiva y j es sobreyectiva.

Definición 7.3.1. Decimos que la sucesión exacta corta $1 \to A \xrightarrow{i} B \xrightarrow{j} C \to 1$ de grupos topológicos abelianos es *bien ajustada* o *split* si

(i) La aplicación i induce un homeomorfismo de A para su imagen

(ii) Existe una función continua τ (que no es necesariamente un homomorfismo) tal que $j\tau = \text{id}_C$.

Notemos que una sucesión exacta corta de grupos abelianos discretos es bien ajustada, así es también una sucesión exacta corta de grupos profinitos abelianos.

Lema 7.3.2.

(a) *Sea* $L \xrightarrow{r} M \xrightarrow{s} N$ *una sucesión exacta de* G*-módulos, y supongamos que existe una función continua* $\kappa : \text{im } r \to L$ *tal que* $r\kappa$ *es la aplicación identidad en* $\text{im } r$*. Entonces la sucesión*

$$C^n(G, L) \xrightarrow{r^*} C^n(G, M) \xrightarrow{s^*} C^n(G, N)$$

de grupos abelianos es exacta.

(b) *Si* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *es una sucesión exacta corta bien ajustada de* G*-módulos, entonces las sucesiones*

(i) $0 \to C^n(G, A) \xrightarrow{i^*} C^n(G, B) \xrightarrow{j^*} C^n(G, C) \to 0$ *y*

(ii) $H^n(G, A) \xrightarrow{i_n} H^n(G, B) \xrightarrow{j_n} H^n(G, C)$

son exactas.

En el siguiente Lema vamos a construir el homomorfismo de conexión.

Lema 7.3.3. *Sea* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *una sucesión exacta corta bien ajustada de* G*-módulos. Para cada* $n \geq 0$ *existe un homomorfismo*

$$d : H^n(G, C) \to H^{n+1}(G, A)$$

tal que la sucesión

$$H^n(G, B) \xrightarrow{j_n} H^n(G, C) \xrightarrow{d} H^{n+1}(G, A) \xrightarrow{i_{n+1}} H^{n+1}(G, B)$$

es exacta. Tal homomorfismo d es llamado el homomorfismo de conexión.

Teorema 7.3.4. *Para cada sucesión exacta corta bien ajustada*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

de G-módulos, existe una correspondiente sucesión exacta larga

$$\begin{aligned} 0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow \cdots \\ \cdots \longrightarrow H^n(G,B) \longrightarrow H^n(G,C) \longrightarrow H^{n+1}(G,A) \longrightarrow \cdots \end{aligned}$$

de grupos de cohomología.

Teorema 7.3.5. (Wilson, J. S., 1997). *Sea $\theta : G_2 \to G_1$ un homomorfismo continuo de grupos profinitos y*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \end{array}$$

un diagrama conmutativo donde la línea superior es una sucesión exacta corta bien ajustada de G_1-módulos y la línea inferior es una sucesión exacta corta bien ajustada de G_2-módulos. Si (θ, α), θ, β y (θ, γ) son pares compatibles entonces el siguiente diagrama

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1^{G_1} & \longrightarrow & B_1^{G_1} & \longrightarrow & C_1^{G_1} & \longrightarrow & H^1(G_1, A_1) \longrightarrow \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A_2^{G_2} & \longrightarrow & B_2^{G_2} & \longrightarrow & C_2^{G_2} & \longrightarrow & H^1(G_2, A_2) \longrightarrow \cdots \end{array}$$

$$\begin{array}{ccccccc} \cdots \longrightarrow & H^n(G_1, B_1) & \longrightarrow & H^n(G_1, C_1) & \longrightarrow & H^{n+1}(G_1, A_1) & \longrightarrow \cdots \\ & \downarrow & & \downarrow & & \downarrow & \\ \cdots \longrightarrow & H^n(G_2, B_2) & \longrightarrow & H^n(G_2, C_2) & \longrightarrow & H^{n+1}(G_2, A_2) & \longrightarrow \cdots \end{array}$$

conmuta (1997: 170).

Sea G un grupo pro-p uniforme finitamente generado y A un G-módulo topológico. Definimos $C^i_{cts}(G,A) = \{f : G^{(i)} \to A \mid f \text{es una función continua}\}$ y la aplicación frontera $\partial^{i+1}_A : C^i(G,A) \to C^{i+1}_{cts}(G,A)$ dada por

$$\begin{aligned} (\partial^{i+1}_A f)(g_1, ..., g_{i+1}) = g_1.f(g_2, ..., g_{i+1}) + \textstyle\sum_{j=1}^{i}(-1)^j f(g_1, ..., g_{j-1}, g_j, g_{j+1}, g_{j+2}, ..., g_{i+1}) \\ +(-1)^{i+1} f(g_1, ..., g_i). \end{aligned}$$

Sean $Z^i_{cts}(G,A) = \ker\partial^{i+1}_A$ y $B^i_{cts}(G,A) = \mathrm{im}\partial^i_A$. Entonces

$$H^i_{cts}(G,A) = Z^i_{cts}(G,A)/B^i_{cts}(G,A)$$

es el **i-ésimo grupo de cohomología continuo** de G con coeficientes en A.

Usando los mismos argumentos como en la prueba del Teorema 7.3.4, obtenemos el siguiente Lema.

Lema 7.3.6. *Sea G un grupo profinito, y sea*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

una sucesión exacta corta de G-módulos topológicos tal que la topología de A es inducida por la topología de B y tal que β es una sección continua (solamente una aplicación continua, no precisa ser un homomorfismo). Entonces existe un homomorfismo de conexión

$$d : H^n_{cts}(G, C) \to H^{n+1}_{cts}(G, A)$$

y obtenemos una sucesión exacta

$$\begin{aligned} 0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{d} H^1_{cts}(G, A) \longrightarrow \cdots \\ \cdots \longrightarrow H^n_{cts}(G, A) \longrightarrow H^n_{cts}(G, B) \longrightarrow H^n_{cts}(G, C) \xrightarrow{d} H^{n+1}_{cts}(G, A) \longrightarrow \cdots \end{aligned}$$

Ahora un resultado sobre la cohomología de grupos pro-p uniformes.

Proposición 7.3.7. *Sea G un grupo pro-p uniforme tal que $\mathbf{L}(G)$ tiene solamente derivaciones internas. Entonces $|H^1_{cts}(G, \mathbf{log}(G))| < \infty$.*

Demostración. Tenemos que G es un grupo pro-p finitamente generado y $\mathbf{L}(G)$ es un $\mathbb{Z}_p$-módulo finitamente generado. Entonces tenemos que $H^1_{cts}(G, \mathbf{log}(G))$ es un $\mathbb{Z}_p$-módulo finitamente generado. Tenemos también que $H^1_{cts}(G, \mathbf{log}(G)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = H^1_{cts}(G, \mathbf{L}(G))$ (P. Symonds and T. Weigel, 2000: 380). Así $H^1_{cts}(G, \mathbf{L}(G)) \cong H^1_{cts}(\mathbf{L}(G), \mathbf{L}(G))$ (P. Symonds and T. Weigel, 2000: 406). Entonces $H^1(\mathbf{L}(G), \mathbf{L}(G)) = \mathrm{Der}(\mathbf{L}(G))/\mathrm{Inn}(\mathbf{L}(G)) = 0$. Luego $H^1_{cts}(G, \mathbf{log}(G)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0$ y así $H^1_{cts}(G, \mathbf{log}(G))$ es un módulo de torsión. Como $H^1_{cts}(G, \mathbf{log}(G))$ es un $\mathbb{Z}_p$-módulo finitamente generado. Entonces $H^1_{cts}(G, \mathbf{log}(G))$ es finito. □

Proposición 7.3.8. *Sea G un grupo pro-p uniforme. Supongamos que el álgebra de Lie $\mathbf{L}(G)$ consiste solamente de derivaciones internas. Entonces existe una constante C tal que*

$$|H^i_{cts}(G, \mathbf{log}(G)/p^i\mathbf{log}(G))| \leq C, \qquad \forall i \geq 1.$$

Demostración. Sea $\varphi : H^2_{cts}(G, \mathbf{log}(G)) \to H^2_{cts}(G, \mathbf{log}(G))$ una aplicación definida por $\varphi(\sigma) = p^i\sigma$. Así $\ker\varphi$ está contenido en el subgrupo de torsión de $H^2_{cts}(G, \mathbf{log}(G))$.

Por otra parte tenemos que G es FP_∞ y $\mathbf{log}(G)$ es un $\mathbb{Z}_p$-módulo finitamente generado. Entonces $H^2_{cts}(G, \mathbf{log}(G))$ es un $\mathbb{Z}_p$-módulo finitamente generado. Luego el subgrupo de torsión de $H^2_{cts}(G, \mathbf{log}(G))$ es finito, llamaremos P a ese grupo. Por la Proposición 7.3.7 $H^1_{cts}(G, \mathbf{log}(G))$ es finito y usando el Lema 7.3.6 tenemos que

$$|H^2_{cts}(G, \mathbf{log}(G))/p^i\mathbf{log}(G))| \leq |H^1_{cts}(G, \mathbf{log}(G))||P| < \infty.$$

□

Capítulo 8

El álgebra de Lie nilpotente de Sato

Este capítulo es esencial para obtener el resultado exigido en el capítulo 9 y posterior consecuencia dada en el capítulo 10, el cuál es el objeto del presente trabajo. El contenido en su totalidad es obtenido del artículo de T. Sato, "The derivations of the Lie algebras" (1971: 21-36), en dicho artículo Sato consigue obtener un álgebra de Lie de dimensión 41 con coeficientes en un cuerpo de característica 0. El teorema principal de este capítulo es el Teorema 8.2.1, que muestra que existe un álgebra de Lie que no posee derivaciones externas y cuyo centro es no trivial.

8.1. Preliminares y notaciones

En palabras de Sato: "A lo largo de este capítulo vamos a suponer que las álgebras de Lie tienen sus coeficientes en un cuerpo de característica 0. Para un subconjunto M de un espacio vectorial, denotamos por $\{M\}$ el subespacio generado por los elementos de M. Cuando M es un subconjunto de un álgebra de Lie L y k es un número natural, denotamos por M^k el subespacio generado por los elementos de la forma

$$[m_1, [m_2, [\dots [m_{k-1}, m_k] \dots] \quad (m_1, m_2, \dots, m_k \in M).$$

Una derivación de un álgebra de Lie L es una transformación lineal de D para D tal que

$$D[x, y] = [Dx, y] + [x, Dy] \qquad x, y \in L$$

Sean D_1 y D_2 dos derivaciones de L. Entonces $[D_1, D_2] = D_1D_2 - D_2D_1$ define un corchete de Lie. Así el conjunto de todas las derivaciones de L forman un álgebra de Lie. Vamos a denotar esta álgebra por $\mathfrak{D}(L)$.

Sea $x \in L$. La aplicación $ad(x) : L \to L$ definida por $(ad(x))(y) = [x, y]$, para todo $y \in L$ es llamada una *derivación interior de* L. El ideal generado por todas las derivaciones interiores es denotado por $\mathfrak{J}(L)$. Sea $Z(L)$ el centro del álgebra de Lie L entonces $\mathfrak{J}(L) \cong L/Z(L)$. Una derivación que no es interior será llamada una *derivación exterior*.

Un álgebra de Lie L es soluble si su serie derivada termina en la subálgebra cero, i.e si existe un $n \in \mathbb{N}$ tal que

$$0 \lhd [L^n, L^n] \lhd \cdots \lhd [L, L] \lhd L$$

El radical de un álgebra de Lie L es el mayor ideal soluble de L. Denotaremos el radical de $\mathfrak{D}(L)$ por $\mathfrak{R}(L)$. Un álgebra de Lie es *simple* si ella es un álgebra de Lie no abeliana cuyos

únicos ideales son el ideal cero y la misma álgebra. Un álgebra de Lie se llama *semi-simple* si ella es la suma directa de álgebras de Lie simples. Denotamos por $\mathfrak{G}(L)$ a la subálgebra semi-simple maximal de $\mathfrak{D}(L)$" (T.Sato, 1971: 22).

Definición 8.1.1. Sea $\mathfrak{D}(R)$ el álgebra de derivaciones de un álgebra de Lie soluble R, y $\mathfrak{G}(R)$ su subálgebra semi-simple maximal. Si existe una derivación externa que es conmutable con todos los elementos de $\mathfrak{G}(R)$, diremos que R *pertenece a la clase* $\mathfrak{D}$. No es difícil mostrar que la definición es independiente de $\mathfrak{G}(R)$.

Sato también menciona que: "Sea L un álgebra de Lie real finito-dimensional. Una *descomposición de Levi* de L es poder escribir L como producto semi-directo de un ideal soluble y una subálgebra semi-simple. El ideal soluble en el producto directo es el radical de L. La subálgebra semi-simple en el producto directo vamos a llamarla *subálgebra de Levi*.

Sea L un álgebra de Lie con las condiciones antes mencionadas. Sea $L = S + R$ una descomposición de Levi de L. Vamos a denotar la restricción de $ad(s)$ para R como $ad_R(s)$. Así $ad_R S = \{ad_R(s) \mid s \in S\}$" (T. Sato, 1971: 31).

Proposición 8.1.2. *Un álgebra de Lie R no posee derivaciones externas si y solo si cualquier derivación de R que es conmutable con todos los elementos de $ad_R S$ es una derivación interna.*

Proposición 8.1.3. *Si el radical R del álgebra de lie L pertenece a la clase $\mathfrak{D}$, entonces L posee una derivación externa.*

Proposición 8.1.4. *Si el álgebra de Lie soluble R es escrito como suma directa de dos ideales R_1 y R_2; y si además R_1 pertenece a la clase $\mathfrak{D}$, entonces R también pertenece a la clase $\mathfrak{D}$.*

Proposición 8.1.5. *Si el álgebra de Lie tiene su centro diferente de cero y no posee derivaciones externas, entonces L no es soluble y su radical es nilpotente; además, $L = [L, L]$.*

Entonces, podemos encontrar muchos ejemplos de álgebras de Lie con derivaciones externas. Pero, ¿qué hay de las álgebras de Lie con centro diferente de cero que no posean derivaciones externas?, ¿existe alguna? En la siguiente sección daremos un ejemplo de tal álgebra de Lie. Para eso, precisamos construir un álgebra de Lie nilpotente que no pertenezca a la clase $\mathfrak{D}$.

8.2. Ejemplo de un álgebra de Lie nilpotente que no pertenece a la clase $\mathfrak{D}$

Este es el resultado más importante del capítulo.

Teorema 8.2.1. (**Sato**). *Existe un álgebra de Lie que no posee derivaciones externas y tiene centro diferente de cero.*

la demostración de Sato es la siguiente: "Para probar el teorema, vamos a construir un álgebra de Lie nilpotente N de dimensión 38, y, además, un álgebra de Lie de dimensión 41 cuyo radical es N. Sean $x_1, x_2, ..., x_{38}$ una base de N, y sea N generado como un álgebra de Lie por los elementos x_1, x_2, x_3 y x_4. El corchete de Lie en N es dada por la siguiente tabla, pero cuando el corchete de Lie no aparece en la tabla consideramos que este es cero.

$$
\begin{array}{lll}
[x_1, x_2] = x_5 & [x_1, x_4] = x_7 & [x_2, x_4] = x_8 \\
[x_1, x_3] = x_6 & [x_2, x_3] = x_7 - x_5 & [x_3, x_4] = x_5
\end{array}
$$

$$
\begin{array}{lll}
[x_1, x_6] = x_9 & [x_2, x_7] = x_{11} & [x_3, x_8] = x_{15} \\
[x_1, x_7] = x_{10} & [x_2, x_8] = x_{12} & [x_4, x_6] = x_{14} \\
[x_1, x_8] = x_{11} & [x_3, x_6] = x_{13} & [x_4, x_7] = x_{15} \\
[x_2, x_6] = x_{10} & [x_3, x_7] = x_{14} & [x_4, x_8] = x_{16}
\end{array}
$$

$$
\begin{array}{lll}
[x_1, x_9] = x_{17} & [x_2, x_{11}] = x_{20} & [x_4, x_{13}] = 30x_{35} \\
[x_1, x_{10}] = x_{18} & [x_2, x_{12}] = x_{21} & [x_4, x_{14}] = 20x_{36} \\
[x_1, x_{11}] = x_{19} & [x_3, x_{13}] = 60x_{34} & [x_4, x_{15}] = 15x_{37} \\
[x_1, x_{12}] = x_{20} & [x_3, x_{14}] = 30x_{35} & [x_4, x_{16}] = 12x_{38} \\
[x_2, x_9] = x_{18} & [x_3, x_{15}] = 20x_{36} & \\
[x_2, x_{10}] = x_{19} & [x_3, x_{16}] = 15x_{37} &
\end{array}
$$

$$
\begin{array}{lll}
[x_1, x_{17}] = x_{22} & [x_3, x_{18}] = x_{29} & [x_6, x_{11}] = -x_{30} \\
[x_1, x_{18}] = x_{23} & [x_3, x_{19}] = x_{30} & [x_6, x_{12}] = -x_{31} \\
[x_1, x_{19}] = x_{24} & [x_3, x_{20}] = x_{31} & [x_7, x_9] = -x_{29} \\
[x_1, x_{20}] = x_{25} & [x_3, x_{21}] = x_{32} & [x_7, x_{10}] = -x_{30} \\
[x_1, x_{21}] = x_{26} & [x_4, x_{17}] = x_{29} & [x_7, x_{11}] = -x_{31} \\
[x_2, x_{17}] = x_{23} & [x_4, x_{18}] = x_{30} & [x_7, x_{12}] = -x_{32} \\
[x_2, x_{18}] = x_{24} & [x_4, x_{19}] = x_{31} & [x_8, x_9] = -x_{30} \\
[x_2, x_{19}] = x_{25} & [x_4, x_{20}] = x_{32} & [x_8, x_{10}] = -x_{31} \\
[x_2, x_{20}] = x_{26} & [x_4, x_{21}] = x_{33} & [x_8, x_{11}] = -x_{32}
\end{array}
$$

$[x_2, x_{21}] = x_{27}$ $[x_6, x_9] = -x_{28}$ $[x_8, x_{12}] = -x_{33}$
$[x_3, x_{17}] = x_{28}$ $[x_6, x_{10}] = -x_{29}$

$[x_1, x_{29}] = x_{34}$ $[x_3, x_{26}] = -x_{37}$ $[x_7, x_{20}] = (1/2)x_{37}$
$[x_1, x_{30}] = x_{35}$ $[x_3, x_{27}] = -x_{38}$ $[x_7, x_{21}] = (4/5)x_{38}$
$[x_1, x_{31}] = x_{36}$ $[x_4, x_{22}] = 5x_{34}$ $[x_8, x_{17}] = -4x_{35}$
$[x_1, x_{32}] = x_{37}$ $[x_4, x_{23}] = 2x_{35}$ $[x_8, x_{18}] = -2x_{36}$
$[x_1, x_{33}] = x_{38}$ $[x_4, x_{24}] = x_{36}$ $[x_8, x_{19}] = -x_{37}$
$[x_2, x_{28}] = -5x_{34}$ $[x_4, x_{25}] = (1/2)x_{37}$ $[x_8, x_{20}] = (-2/5)x_{38}$
$[x_2, x_{29}] = -2x_{35}$ $[x_4, x_{26}] = (1/5)x_{38}$ $[x_9, x_{10}] = -3x_{34}$
$[x_2, x_{30}] = -x_{36}$ $[x_6, x_{18}] = 2x_{34}$ $[x_9, x_{11}] = -3x_{35}$
$[x_2, x_{31}] = (-1/2)x_{37}$ $[x_6, x_{19}] = 2x_{35}$ $[x_9, x_{12}] = -3x_{36}$
$[x_2, x_{32}] = (-1/5)x_{38}$ $[x_6, x_{20}] = 2x_{36}$ $[x_{10}, x_{11}] = -x_{36}$
$[x_3, x_{23}] = -x_{34}$ $[x_6, x_{21}] = 2x_{37}$ $[x_{10}, x_{12}] = (-3/2)x_{37}$
$[x_3, x_{24}] = -x_{35}$ $[x_7, x_{17}] = -4x_{34}$ $[x_{11}, x_{12}] = (-3/5)x_{38}$
$[x_3, x_{25}] = -x_{36}$ $[x_7, x_{18}] = -x_{35}$

Definimos $U = \{x_1, x_2, x_3, x_4\}$. Podemos verificar que el corchete de Lie definido satisface la identidad de Jacobi. Usando el hecho $U^7 = 0$, $[U^2, U^2] = 0$ y que x_5 pertenece al centro de N, podemos también reducir un poco el cálculo.

Ahora vamos a tomar los siguientes endomorfismos lineales de U:

$$\begin{aligned} s_0 &: x_1 \mapsto x_1,\ x_2 \mapsto -x_2,\ x_3 \mapsto x_3,\ x_4 \mapsto -x_4 \\ s_1 &: x_1 \mapsto x_2,\ x_2 \mapsto 0,\ x_3 \mapsto x_4,\ x_4 \mapsto 0 \\ s_2 &: x_1 \mapsto 0,\ x_2 \mapsto x_1,\ x_3 \mapsto 0,\ x_4 \mapsto x_3 \end{aligned}$$

Entonces $\mathfrak{G} = \{s_0, s_1.s_2\}$ forma un álgebra de Lie simple. Vamos a ampliar s_0, s_1, s_2 para derivaciones de N. Esto es posible pues N es descompuesto en una suma directa de $\mathfrak{G}$-módulos invariantes irreductibles como sigue

$$\begin{aligned} N = \ & \{x_1, x_2\} \oplus \{x_3, x_4\} \oplus \{x_5\} \oplus \{x_6.x_7 - (1/2)x_5, x_8\} \oplus \\ & \{x_9, x_{10}, x_{11}, x_{12}\} \oplus \{x_{13}, x_{14}, x_{15}, x_{16}\} \oplus \{x_{17}, x_{18}, x_{19}, x_{20}, x_{21}\} \\ & \oplus \{x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}\} \oplus \{x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}\} \\ & \oplus \{60x_{34}, 30x_{35}, 20x_{36}, 15x_{37}, 12x_{38}\} \end{aligned}$$

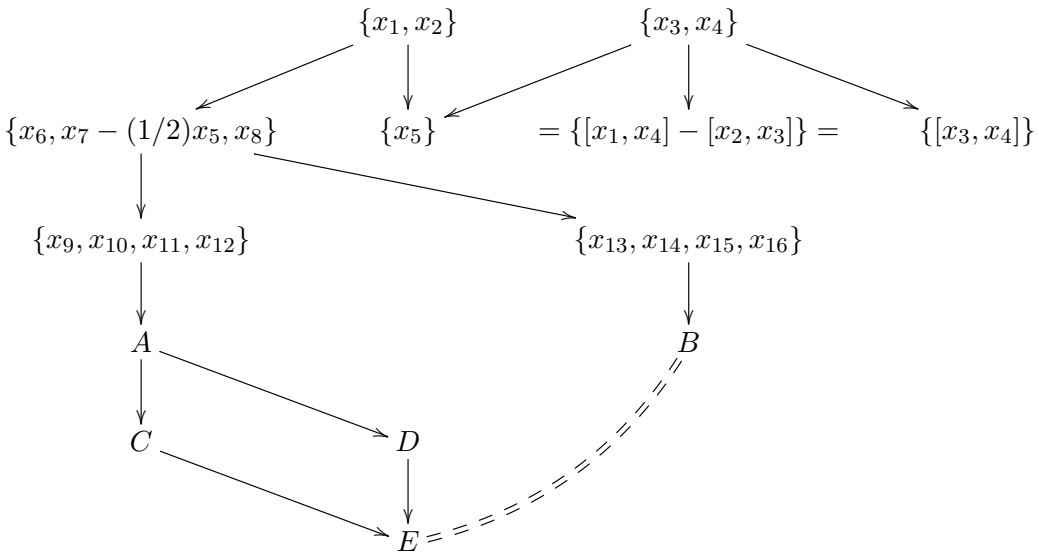
En relación a la operación de $\mathfrak{G}$, N posee la estructura indicada en el siguiente diagrama. Aquí $\{\quad\}$ es un subespacio $\mathfrak{G}$-irreductible, y denotamos por '$\longrightarrow$' el proceso de generación de ideales, y por '===' la identificación de subespacios.

Sean

- $A = \{x_{17}, x_{18}, x_{19}, x_{20}, x_{21}\}$
- $B = \{[x_3, x_{13}], [x_3, x_{14}], [x_3, x_{15}], [x_3, x_{16}], [x_4, x_{16}]\}$
- $C = \{x_{22}, x_{23}, x_{24}, x_{25}, x_{26}, x_{27}\}$
- $D = \{x_{28}, x_{29}, x_{30}, x_{31}, x_{32}, x_{33}\}$

- $E = \{60x_{34}, 30x_{35}, 20x_{36}, 15x_{37}, 12x_{38}\}$

Entonces



Ahora vamos a probar que el álgebra de Lie nilpotente N no pertenece a la clase $\mathfrak{D}$. Sea D una derivación de N conmutable con todos los elementos de $\mathfrak{G}$. No existe un sumando directo de N que sea $\mathfrak{G}$-isomorfo a $\{x_1, x_2\}$ o $\{x_3, x_4\}$ a parte de ellos mismos. Por tanto por el Lema de Schur [1], D debe tener la siguiente forma:

$$\begin{aligned} Dx_1 &= \alpha x_1 + \gamma x_3 & \qquad Dx_3 &= \beta x_3 + \delta x_1 \\ Dx_2 &= \alpha x_2 + \gamma x_4 & \qquad Dx_4 &= \beta x_4 + \delta x_2 \end{aligned}$$

Entonces D actúa sobre N como sigue:

$$\begin{aligned} x_5 &= [x_1, x_2] \to [\alpha x_1 + \gamma x_3, x_2] + [x_1, \alpha x_2 + \gamma x_4] = (2\alpha + \gamma)x_5 \\ x_5 &= [x_3, x_4] \to [\beta x_3 + \delta x_1, x_4] + [x_3, \beta x_4 + \delta x_2] = (2\beta + \delta)x_5 \\ x_5 &= [x_1, x_4] - [x_2, x_3] \to [\alpha x_1 + \gamma x_3, x_4] + [x_1, \beta x_4 + \delta x_2] \\ &\quad -[\alpha x_2 + \gamma x_4, x_3] - [x_2, \beta x_3 + \delta x_1] = (\alpha + \beta + 2\gamma + 2\delta)x_5 \\ x_6 &= [x_1, x_3] \to [\alpha x_1 + \gamma x_3, x_3] + [x_1, \beta x_3 + \delta x_1] = (\alpha + \beta)x_6 \\ x_9 &= [x_1, x_6] \to [\alpha x_1 + \gamma x_3, x_6] + [x_1, (\alpha + \beta)x_6] \\ &\quad = (2\alpha + \beta)x_9 + \gamma x_{13} \\ 0 &= [x_3, x_9] \to [\beta x_3 + \delta x_1, x_9] + [x_3, (2\alpha + \beta)x_9 + \gamma x_{13}] \\ &\quad = \delta x_{17} + 60\gamma x_{34} \end{aligned}$$

Por tanto tenemos

$$\begin{gathered} 2\alpha + \gamma = 2\beta + \delta = \alpha + \beta + 2\gamma + 2\delta \\ \gamma = \delta = 0, \end{gathered}$$

esto implica que $\alpha = \beta$. Entonces,

$$\begin{gathered} x_{13} = [x_3, x_6] \to [\alpha x_3, x_6] + [x_3, 2\alpha x_6] = 3\alpha x_{13} \\ [x_3, x_{13}] \to [\alpha x_3, x_{13}] + [x_3, 3\alpha x_{13}] = 4\alpha [x_3, x_{13}] \\ x_{34} = [x_1, x_{29}] = [x_1, [x_3, [x_1, [x_1, x_4]]]] \to 6\alpha x_{34}. \end{gathered}$$

[1] **Lema de Schur.** *Sea $\phi : L \to \mathfrak{gl}(V)$ irreducible. Entonces el único endomorfismo de V que conmuta con todos los $\phi(x)$ ($x \in V$) son los escalares.*

Como $[x_3, x_{13}] = 60x_{34}$, conseguimos

$$\alpha = \beta = \gamma = \delta = 0, \text{ así } D = 0$$

Por tanto la derivación de N que es conmutable con todos los elementos de $\mathfrak{G}$ es solamente 0, y así N no pertenece a $\mathfrak{D}$. Cuando tomamos la suma semi-directa $\mathfrak{G} + N$, tenemos el centro $\{x_5\}$ que es diferente de cero, y no tenemos derivaciones externas por la Proposición 8.1.2. Por tanto el teorema está probado. Observamos que $[\mathfrak{G} + N, \mathfrak{G} + N] = \mathfrak{G} + N$, como dice la Proposición 8.1.5" (1971: 21-36).

Capítulo 9

p-Grupos finitos con grupo de automorfismos de orden bajo

En este capítulo desarrollaremos el trabajo realizado por González-Sánchez y Jaikin-Zapirain, "Finite p-groups with small automorphism group" (2015). Para eso vamos a hacer uso del álgebra de Lie de dimensión 41 discutida en la sección 8.2 y de los Teoremaa 6.5.3 y 6.5.4, de esta manera podremos obtener un grupo pro-p uniforme también de dimensión 41; esto será necesario para demostrar la existencia de un p-grupo finito no abeliano de orden mayor que el orden de su grupo de automorfismos.

9.1. Teorema de González-Jaikin

Trataré de seguir al pie de la letra la demostración dada por González y Jaikin, apoyándome claro está, en los capítulos que preceden a este: Consideremos el álgebra de Lie $M = \mathfrak{G}+N$ de dimensión 41 construída en la sección 7.2. Vamos a considerar que el álgebra tiene sus coeficientes en el cuerpo $\mathbb{Q}$ que tiene característica 0. Así M es una $\mathbb{Q}$-álgebra de Lie. El álgebra M posee un subanillo M_0 tal que $M = M_0 \otimes_{\mathbb{Z}} \mathbb{Q}$. Sea $L = p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p)$. Entonces $L \cong \mathbb{Z}_p^{41}$ como $\mathbb{Z}_p$-módulo y $[M, M] = [\mathfrak{G} + N, \mathfrak{G} + N] = \mathfrak{G} + N$. Note que

$$\begin{aligned}[L, L] = [p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p), p^2(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p)] &\subseteq p^4(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p) = p^2(p^2 M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p) \\ &= p^2 L.\end{aligned}$$

Así por la sección 6.5 del Capítulo 6 tenemos que L es una $\mathbb{Z}_p$-álgebra de Lie powerful.

Sea $U = \mathbf{exp}(L)$. Entonces U es un grupo pro-p uniforme (Teorema 6.5.1) y $L = \mathbf{log}(U)$ (Observación 5.7.5). Además

$$\begin{aligned}\mathbf{L}(U) &\cong L \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\ &\cong M \otimes_{\mathbb{Q}} \mathbb{Q}_p.\end{aligned}$$

Así obtenemos el siguiente Lema.

Lema 9.1.1. *La $\mathbb{Q}_p$-álgebra de Lie $\mathbf{L}(U)$ tiene dimensión 41, su centro tiene dimensión 1 y $\mathrm{Der}(\mathbf{L}(U))$ consiste solamente de derivaciones internas.*

Sea $U_i = U/U^{p^i}$. Denotemos por $\rho_{i,j} : \mathrm{Aut}(U_i) \to \mathrm{Aut}(U_j)$ (para $i \geq j$), las aplicaciones

$$\rho_{i,j}(\alpha)(uU^{p^j}) = \alpha(uU^{p^i})U^{p^j}, \text{ para todo } \alpha \in \mathrm{Aut}(U_i),\ u \in U.$$

Proposición 9.1.2. *Existe una constante $k \in \mathbb{N}$ tal que, para todo $i \geq 2k$.*

$$\ker\rho_{i,k} \leq \mathrm{Inn}(U_i)\ker\rho_{i,i-k}. \tag{9.1}$$

Demostración. Por la Proposición 7.3.8 existe una constante C tal que

$$|H^1_{cts}(U, \mathbf{log}(U)/p^i\mathbf{log}(U))| \leq C$$

entonces existirá $k \in \mathbb{N}$ tal que $p^k H^1_{cts}(U, \mathbf{log}(U)/p^i\mathbf{log}(U)) = 0$ para todo i. Probaremos esto por inducción sobre i.

Si $i = 2k$, entonces $\ker\rho_{2k,k} \leq \mathrm{Inn}(U_{2k})\ker\rho_{2k,k}$. Ahora supongamos que la proposición sea válida para i. Probaremos la misma para $i+1$. Sea $\phi \in \ker\rho_{i+1,k}$. Del diagrama conmutativo

$$\begin{array}{ccc} \mathrm{Aut}(U_{i+1}) & \xrightarrow{\rho_{i+1,k}} & \mathrm{Aut}(U_k) \\ {\scriptstyle \rho_{i+1,i}}\downarrow & \nearrow_{\rho_{i,k}} & \\ \mathrm{Aut}(U_i) & & \end{array}$$

sigue que $\rho_{i,k}\circ\rho_{i+i,i}(\phi) = \rho_{i+1,k}(\phi) = id_{U_k}$, así $\rho_{i+i,i}(\phi) \in \ker\rho_{i,k}$. Por la hipótesis inductiva tenemos que $\ker\rho_{i,k} \leq \mathrm{Inn}(U_i)\ker\rho_{i,i-k}$, sigue que $\rho_{i+i,i}(\phi) \in \mathrm{Inn}(U_i)\ker\rho_{i,i-k}$ y por tanto $\phi \in \ker\rho_{i+1,i-k}\mathrm{Inn}(U_{i+1})$. Sin pérdida de generalidad, vamos a suponer que $\phi \in \ker\rho_{i+1,i-k}$. Definamos la siguiente función

$$\begin{aligned} s : U &\to U^{p^{i-k}}/U^{p^{i+1}} \\ u &\mapsto \phi(uU^{p^{i+1}})u^{-1}. \end{aligned}$$

Entonces

$$\begin{aligned} s(u_1u_2) &= \phi(u_1u_2U^{p^{i+1}})u_2^{-1}u_1^{-1} \\ &= \phi(u_1U^{p^{i+1}})u_1^{-1}u_1\phi(u_2U^{p^{i+1}})u_2^{-1}u_1^{-1} \\ &= s(u_1)u_1s(u_2)u_1^{-1}. \end{aligned}$$

Así $s \in \mathcal{Z}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Por el Lema 5.7.12, $U^{p^{i-k}}/U^{p^{i+1}}$ es abeliano, pues $i-k \leq i+1 \leq 2(i-k)+1$ y

$$U^{p^{i-k}}/U^{p^{i+1}} \cong \mathbf{log}(U)/p^{k+1}\mathbf{log}(U)$$

como U-módulo. En particular;

$$p^k H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) = 0 \qquad (\text{para } i = k+1)$$

Consideramos la siguiente sucesión exacta de U-módulos:

$$1 \longrightarrow U^{p^{i-k+1}}/U^{p^{i+1}} \xrightarrow{\alpha} U^{p^{i-k}}/U^{p^{i+1}} \xrightarrow{\beta} U^{p^i}/U^{p^{i+1}} \longrightarrow 1$$

donde $\alpha(uU^{p^{i+1}}) = uU^{p^{i+1}}$ y $\beta(uU^{p^{i+1}}) = u^{p^k}U^{p^{i+1}}$. Entonces tenemos que la sucesión

$$H^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}}) \xrightarrow{\alpha^*} H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) \xrightarrow{\beta^*} H^1_{cts}(U, U^{p^i}/U^{p^{i+1}})$$

es exacta por el Lema 7.3.6. Así im $\alpha^* = \ker\beta^* = H^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$. Luego existe $s' \in \mathcal{Z}^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}})$ tal que $\alpha^*(s'\mathcal{B}^1_{cts}(U, U^{p^{i-k+1}}/U^{p^{i+1}})) = s\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$.
De esto sigue que:
$s'\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}}) = s\mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$ y por tanto $(s')^{-1}s \in \mathcal{B}^1_{cts}(U, U^{p^{i-k}}/U^{p^{i+1}})$.
Así podemos obtener un υ en $U^{p^{i-k}}/U^{p^{i+1}}$ tal que para todo $u \in U$ tenemos que $(s')^{-1}(u)s(u) = [\upsilon, u]$ o de igual forma $s(u) = s'(u)\upsilon u\upsilon^{-1}u^{-1}$. Luego obtenemos que

$$\begin{aligned}\phi(uU^{p^{i+1}}) &= s(u)u = s'(u)\upsilon u\upsilon^{-1} \\ &= (s'(u)u)u^{-1}\upsilon u\upsilon^{-1} \\ &= (s'(u)u)[u^{-1}, \upsilon].\end{aligned}$$

Si definimos $\psi(u) = s'(u)u$. No es difícil mostrar que $\psi \in ker\rho_{i+1.i+1-k}$.
Así $\phi \in \ker\rho_{i+1,i+1-k}\mathrm{Inn}(U_{i+1})$. □

Corolario 9.1.3. *Existe una constante D tal que*

$$|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| \leq D \text{ para todo } i.$$

Demostración. Por la proposición anterior y usando el hecho que $\mathrm{Inn}(U_i) \cap \ker\rho_{i,i-k} = id_{U_i}$ tenemos que

$$\begin{aligned}|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| &\leq |\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)\ker\rho_{i,i-k}||\mathrm{Inn}(U_i)\ker\rho_{i,i-k} : \mathrm{Inn}(U_i)| \\ &\leq |\mathrm{Aut}(U_i) : \ker\rho_{i,k}||\ker\rho_{i,i-k}| \leq |\mathrm{Aut}(U_k)||\ker\rho_{i,i-k}|.\end{aligned}$$

Ahora, como $\mathbf{L}(U)$ tiene dimensión 41 sigue que $\mathrm{d}(U) = 41$ y sabiendo que $U_i = U/U^{p^i}$ obtenemos $\mathrm{d}(U_i) = 41$. Además, por (5.3), $|U^{p^{i-k}}/U^{p^i}| = p^{41k}$.

Consideramos $\alpha \in ker\rho_{i,i-k}$ y $uU^{p^i} \in U_i$ entonces $\rho_{i,i-k}(\alpha)(uU^{p^{i-k}}) = \alpha(uU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$, así $\alpha(uU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$. Sea $\alpha(uU^{p^i}) = vU^{p^i}$ para algún $v \in U$ tenemos que $(vU^{p^i})U^{p^{i-k}} = uU^{p^{i-k}}$ y por tanto $v^{-1}u \in U^{p^{i-k}}$. Luego $v^{-1}u = \overline{u} \in U^{p^{i-k}}$ y

$$\alpha(uU^{p^i}) = vU^{p^i} = u\overline{u}^{-1}U^{p^i}, \qquad \text{donde } \overline{u}^{-1}U^{p^i} \in U^{p^{i-k}}/U^{p^i}.$$

Así tenemos que las posibilidades de $\alpha(uU^{p^i})$ son como máximo $|U^{p^{i-k}}/U^{p^i}| = p^{41k}$ y sabiendo que la base tiene 41 elementos obtenemos que $|ker\rho_{i,i-k}| \leq p^{(41)^2k}$ y por tanto

$$|\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)| \leq p^{(41)^2k}.|\mathrm{Aut}(U_k)| = D. \tag{9.2}$$

lo que queríamos probar. □

El resultado principal de este capítulo es demostrar que existe un p-grupo finito no abeliano cuyo orden es mayor que el orden del grupo de sus automorfismos.

Teorema 9.1.4. (González-Jaikin). *Para cada primo p existe una família de p-grupos finitos $\{U_i\}$ tal que*

$$\lim_{i\to\infty} |U_i| = \infty \qquad \text{y} \qquad \lim_{i\to\infty} sup\, \frac{|\mathrm{Aut}U_i|}{|U_i|^{40/41}} < \infty.$$

En particular, para cada primo p, existe un p-grupo finito no abeliano G tal que $|\mathrm{Aut}(G)| < |G|$.

Demostración. Por la Definición 5.6.1 y la Proposición 5.6.4,

$$|U_i| = |U : U^{p^i}| = |U : U^p||U^p : U^{p^2}| \cdots |U^{p^{i-1}} : U^{p^i}| = p^{41}p^{41}\cdots p^{41} = p^{41i}.$$

Así tenemos que

$$\lim_{i\to\infty} |U_i| = p^{41i} = \infty. \tag{9.3}$$

Definimos el siguiente homomorfismo

$$\begin{aligned} \sigma : Z(U) &\to Z(U_i) \\ u &\mapsto uU^{p^i} \end{aligned}$$

Sea $v \in \ker\sigma$. Entonces $v \in Z(U)$ y $v \in U^{p^i}$. Así $\ker\sigma \subseteq Z(U) \cap U^{p^i}$. Ahora consideramos w en la intersección $Z(U) \cap U^{p^i}$. Luego $Z(U) \cap U^{p^i} \subseteq \ker\sigma$. Entonces por el primer teorema de isomorfismo de grupos tenemos que

$$\frac{Z(U)}{Z(U) \cap U^{p^i}} \leq Z(U_i),$$

y por el segundo teorema de isomorfismo de grupos $Z(U)/Z(U) \cap U^{p^i} \cong U^{p^i}Z(U)/U^{p^i}$. Por otro lado $\mathrm{Inn}U_i \cong U_i/Z(U_i)$. Así tenemos que

$$|\mathrm{Inn}(U_i)| = |U_i/Z(U_i)| = \frac{|U/U^{p^i}|}{|Z(U_i)|} \leq \frac{|U/U^{p^i}|}{|U^{p^i}Z(U)/U^{p^i}|} = |U/U^{p^i}Z(U)|. \tag{9.4}$$

La última igualdad es usando el tercer teorema de isomorfismo de grupos.

Como $\dim(Z(U))$=1 y $\dim(U) = 41$, entonces $\dim(U/Z(U))$=40. Así Tenemos que

$$|(U/Z(U))/(U/Z(U))^{p^i}| = p^{40i}$$

usando otra vez los teoremas de isomorfismo obtenemos

$$|U/U^{p^i}Z(U)| = |(U/Z(U))/(U/Z(U))^{p^i}| = p^{40i}. \tag{9.5}$$

De (9.4) y (9.5) obtenemos que

$$|\mathrm{Inn}U_i| \leq |U/U^{p^i}Z(U)| = p^{40i}$$

y por el Corolario 9.1.3 tenemos

$$\begin{aligned} |\mathrm{Aut}(U_i)| &= |\mathrm{Aut}(U_i) : \mathrm{Inn}(U_i)||\mathrm{Inn}(U_i)| \\ &\leq Dp^{40i} \end{aligned}$$

siendo D la constante en (9.2). De esto sigue que

$$\frac{|\mathrm{Aut}(U_i)|}{|U_i|^{40/41}} \leq \frac{Dp^{40i}}{p^{40i}} = D.$$

Vamos a suponer que para todo i tenemos que $|U_i| \leq |\mathrm{Aut}(U_i)|$, entonces

$$|U_i|^{1/41} = \frac{|U_i|}{|U_i|^{40/41}} \leq \frac{|\mathrm{Aut}(U_i)|}{|U_i|^{40/41}} \leq D, \tag{9.6}$$

lo que contradice (9.3). Esto termina la demostración. □

Capítulo 10

Sobre la Conjetura de Bray-Wilson

En el presente capítulo comprobaremos la existencia de un grupo finito nilpotente en el que el orden de su grupo de automorfismos es menor que el orden de él mismo. También se construirá la prueba que desmiente la conjetura de Bray-Wilson, para un grupo finito supersoluble no nilpotente. Tanto la comprobación de la existencia del grupo finito nilpotente como la prueba que desmiente la conjetura de Bray-Wilson fueron planteadas por González-Sánchez y Jaikin-Zapirain en su artículo titulado "Finite p-groups with small automorphism group" (2015). Seguiremos las indicaciones y relaizaremos los cálculos necesarios para tales fines.

10.1. Un grupo finito nilpotente con grupo de automorfismos de orden bajo

Como cada p-grupo finito es nilpotente (Teorema 4.4.1), entonces tomando la familia $\{U_i\}$ del Teorema 9.1.4 obtenemos que para cada i

$$\frac{|\mathrm{Aut}(U_i)|}{|U_i|^{40/41}} \leq D, \tag{10.1}$$

siendo D la constante dada en (9.2). Luego

$$\phi(|U_i|) = \phi(p^{41i}) = (p-1)p^{41i-1} = \frac{p-1}{p}p^{41i} = \frac{p-1}{p}|U_i| \geq \frac{1}{2}|U_i|. \tag{10.2}$$

De (9.3) y (10.2) Tenemos que

$$\lim_{i\to\infty} \phi(|U_i|) = \infty, \tag{10.3}$$

y usando (10.1) y (10.2)

$$\frac{|\mathrm{Aut}(U_i)|}{\phi(|U_i|)^{40/41}} \leq 2^{40/41}D. \tag{10.4}$$

Supongamos que para todo i, $|\phi(|U_i|)| \leq |\mathrm{Aut}(U_i)|$. Entonces

$$\phi(|U_i|)^{1/41} = \frac{\phi(|U_i|)}{\phi(|U_i|)^{40/41}} \leq \frac{|\mathrm{Aut}(U_i)|}{\phi(|U_i|)^{40/41}} \leq 2^{40/41}D, \tag{10.5}$$

contradiciendo (10.3).

Concluimos que debe existir un grupo finito nilpotente N tal que

$$|\mathrm{Aut}(N)| < \phi(|N|).$$

10.2. Conjetura de Bray-Wilson

En el cuaderno de Kourovka (2010), el matemático rumano Deaconescu plantea las siguientes dos interrogantes: (1) ¿para cada grupo finito G se cumple que $|\mathrm{Aut}(G)| \geq \phi(|G|)$?, (2) ¿si $|\mathrm{Aut}(G)| = \phi(|G|)$ entonces G es cíclico? (2018: 225). John. N. Bray y Robert A. Wilson, respondieron a ambas preguntas en forma negativa (2005), mostrando además que $|\mathrm{Aut}(G)|/\phi(|G|)$ puede hacerse tan pequeño como se desee. comprobando ellos mismos en un artículo posterior (2006) que estos resultados siguen siendo verdaderos si G se considera un grupo perfecto o soluble, permaneciendo el problema abierto cuando G es un grupo supersoluble no nilpotente. Por lo que ellos enunciaron la siguiente conjetura (2006):

Conjetura 10.2.1. (Bray-Wilson). *Si G es un grupo finito supersoluble no nilpotente, entonces* $|\mathrm{Aut}G| > \phi(|G|)$.

Sea p un primo distinto de 2 y 3. Tomemos la familia de p-grupos finitos $\{U_i\}$, considerados en el Teorema 9.1.4. y realicemos el siguiente producto directo

$$H_i = D_3 \times U_i$$

siendo D_3 el grupo diédrico de orden 3. Así obetenemos una nueva familia de grupos $\{H_i\}$. Por el Lema 4.3.12 tenemos que H_i no es nilpotente para cada i, pues D_3 no lo es.

Para cada i, tenemos los siguientes subgrupos maximales de H_i: $\mathbb{Z}_2 \times U_i$, $\mathbb{Z}_3 \times U_i$, $D_3 \times N_i$, con $|N_i| = p^{41i-1}$, de índices 3, 2 y p respectivamente. Así, por la Proposición 4.6.2 (iv), H_i es supersoluble para cada i. Además

$$\begin{aligned}
|\mathrm{Aut}(H_i)| &= |\mathrm{Aut}(D_3 \times U_i)| \\
&= |\mathrm{Aut}(D_3)||\mathrm{Aut}(U_i)| \qquad \text{(Teorema 3.2, Bidwell/ Teorema 1.2, Curran)} \\
&= |D_3||\mathrm{Aut}(U_i)| \\
&= 6 \cdot |\mathrm{Aut}(U_i)| \\
&\leq 6 \cdot D \cdot p^{40i}
\end{aligned}$$

siendo D la constante dada en (9.2).

Por otro lado, tenemos que $\phi(|H_i|) = \phi(|D_3 \times U_i|) = \phi(|D_3|)\phi(|U_i|) = 2 \cdot (p-1) \cdot p^{41i-1}$, y por tanto

$$\frac{|\mathrm{Aut}(H_i)|}{\phi(|H_i|)} \leq \frac{6pDp^{40i}}{2(p-1)p^{41i}} = \frac{3pD}{(p-1)p^i} \longrightarrow 0$$

De esta manera, debe existir un H_k para algún k, tal que $|\mathrm{Aut}(H_k)| < \phi(|H_k|)$. Contradiciendo la Conjetura.

Referencias

Baumslag, G. (1959). *Wreath products and p-groups (pp. 224-231)*. Proc. Camb. Philos. Soc. 55. MR0105437.

Bidwell, J. N. S., Curran, M. J., & McCaughan, d. j. (2006). *Automorphisms of direct products of finite groups (pp. 481-489)*. Archiv der Mathematik. 86.

Bray, J. N., & Wilson, R. A. (2005). *On the orders of automorphism groups of finite groups (pp. 381-385)*. Math. Soc. **37**. Bull. Lond.

Bray, J. N., & Wilson, R. A. (2006). *On the orders of automorphism groups of finite groups II (pp. 537-545)*. J. Group Theory **9**.

Brown, K. S. (1987). *Finiteness properties of groups (pp. 45-75)*, Journal of Pure and Applied Algebra. 44. North Holland.

Buckley, J. (1975/76). *Automorphism groups of isoclinic p-groups (pp. 37-44)*. **12** (1975/76).J. Lond. Math. Soc (2).

Caicedo, J. D. V. (1993). *La conjetura de Serre sobre la multiplicidad de la intersección de dos módulos*, Revista de la Facultad de Ciencias, Universidad Nacional de Colombia, Seccional Medellín. No. 3.

Clement, A. E., Majewicz, S., & Zyman, M. (2017). *The Theory of Nilpotent Groups*. Birkhäuser Basel. Springer International Publishing AG.

Conrad, K. *Subgroup Series II*, Section 4.

Cook, G. C. (2010). *On Profinite Groups of Type FP_∞*. Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK.

Craven, D. A. (2008). *The Theory of p-Groups*. Hilary Term.

Curran, M. J. (2009). *Automorphisms of products of finite groups*. Groups St Andrews 2009 in Bath Volume 1. University of Otago, PO Box 56, Dunedin, New Zealand.

Davitt, R. M. (1970). *The automorphism group of a finite metacyclic p-group (pp 876-879)*. **25**. Proc. Amer. Math. Soc.

Davitt, R. M. (1972). *The automorphism group of finite p-abelian p-groups (pp. 76-85)*. **16**. Illinois J. Math.

Davitt, R. M. (1980). *On the automorphism group of a finite p-group with a small central quotient (pp. 1168-1176)*, **32**. Canad. J. Math.

Davitt, R. M., & Otto, A. D. (1971). *On the automorphism group of a finite p-group with the central quotient metacyclic (pp. 467 -472).* **30**. Proc. Amer. Math. Soc.

Davitt, R. M., & Otto, A. D. (1972). *On the automorphism group of a finite modular p-group (pp. 399-404).* **35**. Proc. Amer. Math. Soc.

Dixon, J., Sautoy, M. du., Mann, A., & Segal, D. (1999). *Analytic Pro-p Groups*, 2nd edn. Cambrifge University Press. Cambridge.

Dummit, D. S., & Foot, R. M. (2004). *Abstract Algebra.* **PH**. John Wiley & Sons, Inc.

Eick, B. (2006). *Automorphism groups of* 2*-groups (pp. 91-101).* **300**. J. Algebra.

Exarchakos, T. (1981). *LA-groups (pp. 185-190).* **33**. J. Math. Soc. Japan.

Exarchakos, T. (1989). *On p-groups of small order (pp 73-76).* **45**(59). Publ. Inst. Math. Beograd. N.S.

Faudree, R. (1968). *A note on the automorphism group of a p-group (pp. 1379-1382).* **19**. Proc. Amer. Math. Soc.

Fernández-Alcober, G. A. *An introduction to finite p-groups: regular p-groups and groups of maximal class*, XVI Escola de Álgebra. Brasilia. 2000.

Fried, M. D., & Jarden, M. (2004). *Field Arithmetic.* A Series of Modern Surveys in Mathematics. Second Edition.

Fouladi, S., Jamali, A. R., & Orfi, R. (2007). *Automorphism groups of finite p-groups of coclass* 2 *(pp. 437-440).* **10**. J. Group Theory.

Gavioli, N. (1993). *The number of automorphisms of groups of order* p^7 *(pp. 177-184).* **93**. Proc. R. Irish Acad. Sect. A.

Gaschütz, W. (1965). *Kohomologische Trivialitäten und äussere Automorphismen von p-Gruppen (pp. 432 -433).* **88**. Math. Z.

González-Sánchez, & Jaikin-Zapirain. (2015). *Finite p-groups with small automorphism group (Vol.3, e7, 11 pages).* Forum of Mathematics, Sigam.

Hummel, K. G. (1975). *The order of the automorphism group of a central product (pp. 37-40).* Proc. Amer. Math. Soc. 47.

Humphreys, J. E. (1970). *Introduction to Lie Algebras and Representation Theory.* Third Printing, Revised. Springer-Verlag. AMS Subject Classification.

Klopsch, B. (2007). *Five lectures on analytic pro-p groups: a meeting-ground between finite p-groups and Lie theory.* University of Oxford.

Lazard, M. (1965). *Groupes analytiques p-adiques (389-603).* **26**. Publ. Math. Inst. Hautes Études Sci.

Lubotzky, A., & Mann, A. (1987). *Powerful p-Groups. II. p-Adic Analytic Groups (pp. 506-515).* **105**. Journal of Algebra.

Mazurov, V. D. & Khukhro, E. I. (2010). *The Kourovka Notebook. Unsolved Problems in Group Theory*. 17th augmented edn. Russian Academy of Sciences Siberian Division, Institute of Mathematics.

Neukirch, J., Schmidt, A., & Wingberg, K. (2008). *Cohomology of Number Fields*. 2nd edn, Grundlehren der Mathematischen Wissenschaften, 323. Springer, Berlin.

Nikolov, N., & Segal, D. (2007). *On finitely gerated profinite groups, I: strong completeness and uniform bounds (pp. 171-238)*. **165**. Annals of Mathematics.

Otto, A. D. (1996). *Central automorphisms of a finite p-group (pp. 280-287)*. **125**. Trans. Amer. Math. Soc.

Ree, R. (1958). *The existence of outer automorphisms of some groups II (pp. 105-109)*. **9**. Proc. Amer. Math. Soc.

Sato, T. (1971). *The derivations of the Lie algebras (pp. 21-36, volume 11, 2000)*. J. **23**. Tôhoku Math.

Sautoy, M. d., Segal, D., & Shalev, A. (2000). *New Horizons in pro-p Groups*. Progress in Mathematics, Vol. 184. Springer.

Schenkman, E. (1955). *The existence of outer automorphisms of some nilpotent groups of class 2 (pp. 6-11)*. **6**. Proc. Amer. Math. Soc.

Sylow, L. (1872). *Théorèmes sur les groupes de subtitutions (584-594)*. Methamtische Annalen **5**.

Symonds, P., & Weigel, T. (2000). *Cohomology of p-adic analytic groups (pp. 349-410)*. New Horizons in Pro-p Groups. Progress in Mathematics, 184. Birkhäuser, Boston, MA.

Thillaisundaram, A. (2012). *The automorphism group for p-central p-groups (pp. 59-71)*. **1**. Int. J. Group Theory.

Wilson, J. S. (1997). *Profinite Groups*. School of Mathematics and Statistics. University of Birmingham.

Yadav, M. K. (2007). *On automorphisms of finite p-groups (pp. 859-866)*. Group Theory **10**.